

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 14-10-2010		2. REPORT TYPE Doctoral Dissertation		3. DATES COVERED (From - To) Feb 2008 – Oct 2010	
4. TITLE AND SUBTITLE Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Caudle, Daryl L.			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Phoenix, School of Advanced Studies 4615 E. Elwood Street Phoenix, AZ 85040			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of the Chairman of the Joint Chiefs of Staff 5000 Joint Staff Pentagon Strategic Plans and Policy (J5) Washington, DC 20318-5000			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) SR 10-00144		
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Unlimited Distribution					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The nation's critical infrastructure, information systems, and telecommunication networks are vulnerable and threatened by an ever-growing number of attacks in cyberspace. An essential element of the nation's comprehensive approach to cybersecurity is the ability for the Department of Defense to protect and defend its information enterprise. Unfortunately, decision-making uncertainty experienced by military leaders when determining the appropriate response to a cyber attack can impede cybersecurity efforts. This qualitative, phenomenological study was used to explore the perceptions and lived experiences of 21 senior military officers serving in cyber warfare divisions for the Chairman of the Joint Chiefs of Staff in Washington, DC. The synthesis of 10 key themes that were exposed during the phenomenological reduction analysis indicated that the decision-making uncertainty experienced by the participants following a cyber attack was described by five interdependent characteristics: (a) response process, (b) human factors, (c) governance, (d) technology, and (e) environment. These interrelated characteristics are similar to the factors found in the literature that describe organizational change uncertainty. The study further indicated the response decision-making process used by senior military officers following a cyber attack was best described by poliheuristic, noncompensatory decision theory. Recommendations for leadership were centered on policy and strategic changes, improving senior officer experience and situational awareness, and enhancing collaboration and coordination among the U.S. government departments and agencies.					
15. SUBJECT TERMS Cyberspace, cyber, use of force, cybersecurity, uncertainty, poliheuristic, decision-making, organizational change, phenomenological, response process, human factors, governance, technology, environment, cyberpower, deterrence, warfare, strategy, policy, legal framework, leadership					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NUMBER 482	19a. NAME OF RESPONSIBLE PERSON David A. Hoopes, LtCol, USAF
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (include area code) (703) 697-2137

**DECISION-MAKING UNCERTAINTY AND THE USE OF FORCE
IN CYBERSPACE:
A PHENOMENOLOGICAL STUDY OF MILITARY OFFICERS**

by

Daryl L. Caudle

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Management in Organizational Leadership

UNIVERSITY OF PHOENIX

October 2010

© 2010 by DARYL L. CAUDLE
ALL RIGHTS RESERVED

DECISION-MAKING UNCERTAINTY AND THE USE OF FORCE

IN CYBERSPACE:

A PHENOMENOLOGICAL STUDY OF MILITARY OFFICERS

by

Daryl L. Caudle

October 2010

Approved:

Craig Barton, Ph.D., Mentor

Steve Seteroff, DBA, Committee Member

Barry Spiker, Ph.D., Committee Member

Accepted and Signed:

Craig Barton

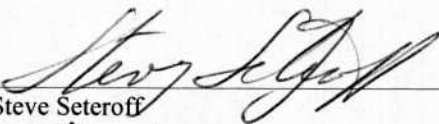


October 15, 2010

Date

Accepted and Signed:

Steve Seteroff

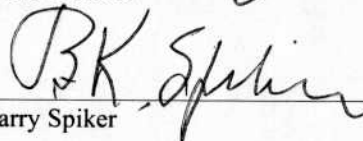


October 15, 2010

Date

Accepted and Signed:

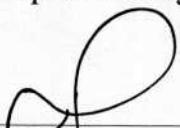
Barry Spiker



October 15, 2010

Date

Jeremy Moreland, Ph.D.
Dean, School of Advanced Studies
University of Phoenix



October 31, 2010

Date

Abstract

The nation's critical infrastructure, information systems, and telecommunication networks are vulnerable and threatened by an ever-growing number of attacks in cyberspace. An essential element of the nation's comprehensive approach to cybersecurity is the ability for the Department of Defense to protect and defend its information enterprise. Unfortunately, decision-making uncertainty experienced by military leaders when determining the appropriate response to a cyber attack can impede cybersecurity efforts. This qualitative, phenomenological study was used to explore the perceptions and lived experiences of 21 senior military officers serving in cyber warfare divisions for the Chairman of the Joint Chiefs of Staff in Washington, DC. The synthesis of 10 key themes that were exposed during the phenomenological reduction analysis indicated that the decision-making uncertainty experienced by the participants following a cyber attack was described by five interdependent characteristics: (a) response process, (b) human factors, (c) governance, (d) technology, and (e) environment. These interrelated characteristics are similar to the factors found in the literature that describe organizational change uncertainty. The study further indicated the response decision-making process used by senior military officers following a cyber attack was best described by poliheuristic, noncompensatory decision theory. Recommendations for leadership were centered on policy and strategic changes, improving senior officer experience and situational awareness, and enhancing collaboration and coordination among the U.S. government departments and agencies.

Dedication

I dedicate this study to my loving wife and best friend, Donna. This dissertation, the culmination of my doctoral journey, was touched in so many ways by your thought provoking recommendations, inspirational insights, and extraordinary understanding. Through your endless patience, tireless support, and unwavering encouragement, you have made me a more effective leader, enlightened scholar, dedicated practitioner, caring father, giving husband, and most of all, a better man. Although the effort and time consumed by this dissertation can never be recaptured, know forever that I am eternally grateful that you were by my side.

Acknowledgments

Many talented, dedicated, and caring leaders, colleagues, peers, and friends supported my doctoral journey. Each added a unique perspective and special value to my work and life in extraordinary and unimaginable ways. To each of you, my most sincerest and heart-felt thank you. To my mother and father for their love, Christian beliefs, and moral standards. To my stepdaughter, Haley for missing so many weekends going shopping and to the movies.

To Dr. Craig Barton, my mentor, and Dr. Steve Seteroff and Dr. Barry Spiker, my committee members, for your sage advice and insightful recommendations that ensured my research study was conducted to the highest scholarly level. To the faculty and staff of the University of Phoenix, especially Dr. Richard Schuttler, Dr. Genevieve Segol, Dr. Rita Hartman, and Dr. Kimberly Blum for your enlightened guidance and experienced suggestions that taught me how to conduct research. To my University of Phoenix classmates and teammates, especially Dr. Glenda Holcomb for leading the way and providing me with invaluable advice, best practices, and lessons learned.

To the Joint Staff for allowing me to conduct this research study using the most professionally competent military officers in the world. A special thank you to the Information and Cyberspace Policy Division within the J5 Directorate for working closely with me to ensure this research study made a significant and substantial contribution to the body of knowledge. Without the dedicated and professional support of Brig Gen Michele Johnson, Senior Executive Teresa Salazar, Col Pete Kim, Col Mike Barry, Lt Col Dave Hoopes, LCDR Dave Burke, and LCDR Ed Byers, this research study would not have been possible.

Disclaimer

The views presented in this dissertation are those of the author or the research participants and do not necessarily represent the views of the Department of Defense or its Components or any U.S. government department or agency.

Table of Contents

List of Tables.....	xviii
List of Figures	xix
Chapter 1: Introduction	1
Background of the Problem.....	2
Statement of the Problem	9
Purpose of the Study	10
Significance of the Study	11
Significance of the Study to Leadership	13
Nature of the Study	14
Appropriateness of the research method.....	15
Appropriateness of the research design.	19
Other qualitative research designs considered.	21
Ethnography.	21
Case study.	22
Delphi technique.	22
Grounded theory.....	23
Research Question.....	24
Theoretical Framework	26
Compensatory decision-making models.	26
Noncompensatory decision-making models.	28
Complexity theory.....	30
Cyberpower theory.....	30

Cyber deterrence theory.....	31
Definition of Terms	34
Assumptions	35
Scope	35
Limitations	36
Delimitations	37
Summary	38
Chapter 2: Review of the Literature.....	40
Documentation	41
Review of the Literature Strategy	42
Theoretical Framework	44
Historical Perspective.....	46
History of the Internet: Building the Digital Battlefield	47
Computer networks.	47
ARPANET.	49
Internet.	50
World Wide Web.	52
History of Cyberspace.....	54
Origins.....	55
Cyberspace recognized nationally.	55
Cyberspace as a new warfighting domain.....	56
Cyber Warfare	57
Background.	58

Cyberpower theory.....	60
Social and cultural aspects.	64
Behavioral and cognitive aspects.....	66
Ethical aspects.....	68
Technical aspects.	70
Traditional versus Cyber Warfare Doctrine	71
Command and control.....	71
Intelligence.....	72
Fires.....	72
Movement and maneuver.....	73
Protection.	74
Sustainment.....	75
Traditional warfighting decision-making.....	76
Defensive response action thresholds (“Red lines”).	77
Effects-Based warfare.	79
Cyberspace Operations.....	81
Computer network operations (CNO).....	81
Computer network attack (CNA).....	82
Computer network defense (CND).	84
Computer network exploitation (CNE).....	85
Cyber crime.....	86
Economic impact of cyber crime.	88
Cyber terrorism.	89

Nation state actors.....	92
Non-Nation state actors.....	94
Cyber threats.	95
Cyber vulnerabilities.	98
Attribution challenges.	100
Decision-Making under Risk, Uncertainty, and Ignorance.....	102
The Military Decision-Making Process (MDMP)	104
Decision Theory	106
Decision theory background.	106
Decision strategies.	108
Compensatory decision theory.....	109
Noncompensatory decision theory.....	110
Poliheuristic decision theory.....	111
Cybernetic decision theory.....	112
Utility theory.	113
Prospect theory.....	114
Regret theory.....	116
Game theory.....	118
Bargaining theory.....	120
“OODA” loop theory.	122
Complexity Theory	126
Systems theory.	127
Cybernetics.....	129

Chaos theory.	130
Catastrophe theory.	132
Deterrence Theory.....	134
Traditional deterrence theory.	134
Cyber deterrence theory.	137
Schmitt Decision Analysis	141
Legal Aspects of Cyber Warfare.....	144
International law.	145
North Atlantic Treaty applicability.	148
Rules of engagement and inherent right of self-defense.....	150
Examples of Cyber Attacks.....	152
Estonia.....	152
Georgia.....	154
Pentagon.....	155
Conclusions	157
Historical perspective.....	157
Cyber versus traditional warfare operations.	158
Decision theory.	159
Complexity and uncertainty theories.	161
Deterrence theory framework.	162
Legal aspects of cyber warfare.....	163
Limitations and Gaps in the Research Literature	164
National policy and legal frameworks.	165

Leadership paradigms.	166
Decision-Making processes.	167
Summary	168
Chapter 3: Method.....	170
Research Method.....	172
Appropriateness of Design	178
Other Qualitative Research Designs Considered	182
Research Question.....	190
Population.....	191
Sampling Frame	191
Informed Consent.....	193
Confidentiality.....	195
Geographic Location	196
Data Collection.....	197
Instrumentation.....	202
Validity and Reliability	205
Validity.....	205
Reliability.....	208
Expert panel review.	209
Pilot study considerations.	210
Data Analysis	211
Summary	215
Chapter 4: Results	217

Expert Panel Review	218
Sample Demographics.....	220
Data Collection Process	227
Interview process.	227
Transcription process.	229
Data Analysis and Presentation of Findings	231
Listing and preliminary grouping.	233
Reduction and elimination.	235
Clustering and thematizing the invariant constituents.	236
Final identification of the invariant constituents and themes.	237
Theme 1: Response characteristics and efficacy considerations.....	238
Theme 2: Social, behavioral, cultural, and cognitive aspects.	238
Theme 3: Policy and strategic aspects.....	239
Theme 4: Legal and ethical aspects.....	239
Theme 5: Organizational concepts, constructs, and relational considerations.....	240
Theme 6: Data, information, and technology considerations.....	240
Theme 7: Cyber attack characteristics.	241
Theme 8: Cyber warfare characteristics.....	241
Theme 9: Cyberspace characteristics.	241
Theme 10: Experience, training, and education considerations.....	242
Individual textual descriptions.	242
Individual structural descriptions.....	243

Composite descriptions.....	243
Textural-Structural synthesis.....	244
Summary	245
Chapter 5: Conclusions and Recommendations.....	247
Scope	249
Limitations	249
Delimitations	250
Conclusions	251
Response process.....	253
Response characteristics and efficacy considerations.....	253
Cyber attack characteristics.....	254
Cyber warfare characteristics.....	255
Human factors.....	256
Social, behavioral, cultural, and cognitive aspects.....	257
Experience, training, and education considerations.....	259
Governance.....	259
Policy and strategic aspects.....	260
Legal and ethical aspects.....	261
Technology.....	263
Data, information, and technology considerations.....	263
Environment.....	264
Organizational concepts, constructs, and relational considerations.....	265
Cyberspace characteristics.....	265

Structural Framework for Understanding Decision-Making Uncertainty.....	267
Structural framework.	267
Poliheuristic decision-making process.....	270
Implications	271
Implications for the Department of Defense.....	272
Implications for the National Security Council.	274
Significance of the Study	275
Significance to Leadership	277
Recommendations for Leaders and Stakeholders	278
Recommendations for Department of Defense Leaders.	279
Recommendations for National Security Council Leaders.....	280
Recommendations for Further Research	282
Validating the results off the current study.....	282
Addressing deficiencies in the literature.....	283
Researcher’s Reflections	285
Summary	287
References	289
Appendix A: Review of the Literature Key Search Terms	349
Appendix B: Computer Network Attack Methods.....	352
Appendix C: Characteristics of Decision Strategies	354
Appendix D: Use of Force Analysis Spectrum	356
Appendix E: Letter of Solicitation and Full Disclosure.....	358
Appendix F: Informed Consent Form	360

Appendix G: Joint Staff Interview Permission Form.....	362
Appendix H: Interview Data Collection Form.....	364
Appendix I: Permission to Reuse Copyrighted Sources	367
Appendix J: Rank Order of Invariant Constituents.....	382
Appendix K: Key Themes and Supporting Invariant Constituents.....	388
Appendix L: Individual Textual Descriptions.....	394
Appendix M: Individual Structural Descriptions	423
Appendix N: Composite Textual and Structural Descriptions.....	439
Appendix O: Textual-Structural Synthesis	452
Appendix P: Report Documentation Page	461

List of Tables

Table 1 <i>Participants' Age Distribution</i>	222
Table 2 <i>Participants' Military Rank Distribution</i>	223
Table 3 <i>Participants' Military Service Branches</i>	224
Table 4 <i>Participants' Joint Staff Directorate Codes</i>	225
Table 5 <i>Participants' Years of Military Experience</i>	226
Table 6 <i>Participants' Years of Cyber Warfare Experience</i>	227
Table 7 <i>Key Themes</i>	237

List of Figures

<i>Figure 1.</i> Research strategy for conducting the review of the literature.....	43
<i>Figure 2.</i> Theoretical framework based on Drucker's (2007) five elements of effective decision-making.	45
<i>Figure 3.</i> Boyd's (1986) original OODA loop model.....	123
<i>Figure 4.</i> Boyd's (1996) modified OODA loop model.....	124
<i>Figure 5.</i> Decision tree for determining legal response actions.....	148
<i>Figure 6.</i> Theoretical saturation of thematic data occurred after 18 interviews as verified during the horizontalization process of the phenomenological reduction analysis.	232
<i>Figure 7.</i> Conceptual model representing the factors influencing decision-making uncertainty following a cyber attack with ranked themes shown in parentheses.	252
<i>Figure 8.</i> Leavitt's (1965) Diamond for modeling organizational change.	268
<i>Figure 9.</i> Radnor's (1999) modified Leavitt Diamond applied to the interdependent factors representing the decision-making uncertainty senior military officers experience following a cyber attack.....	269

Chapter 1: Introduction

Information warfare has been in existence since 6th century B.C. when Sun Tzu emphasized the importance of information superiority and asymmetric warfare in *The Art of War* (Addinall, 2004; Mazanec, 2009). More than 2500 years later, as the Internet was beginning to emerge, Post (1979) introduced the concept of *Cybernetic War* (later shortened to cyber war) as the use of computers and computer networks to conduct warfare in cyberspace. By 1996, CIA Director Deutch elevated cyber warfare in the information age to the national level while testifying at a congressional hearing with the statement, “The electron is the ultimate precision guided weapon” (Correll, 1996, p. 2). Deutch’s statement was in response to Senator Nunn’s question about “whether or not foreign governments have sponsored information attacks on our infrastructure” as Nunn opined the possibility of a “Cyber Pearl Harbor” (Correll, 1996, p. 2). Given the real and ever-growing threat of such an event, President G. W. Bush (2003) warned, “Cyber attacks on information networks can have serious consequences such as disrupting critical operations, causing loss of revenue, intellectual property, or life” (p. ix).

Countering such attacks, according to President Bush (2003), requires innovative and effective technologies capable of reducing vulnerabilities coupled with the rules of engagement that support rapid decision-making processes, including the *use of force*. Cyber attacks against Estonia in 2007 as well as Lithuania and Georgia in 2008 are recent examples where nation state leaders (e.g., Presidents, Secretaries, and Ministers of Defense) could not overcome the uncertainty associated with responding to these attacks with a proportional use of force (Lewis, 2007; Rhodin, 2008; Shachtman, 2008). Unfortunately, the United States is just as likely to encounter a cyber attack against the

information systems that support critical infrastructures and military command and control networks (Pace, 2006a; Shea, 2003; Willemssen, 2000). Therefore, without a comprehensive and integrated approach to cyber warfare, the nation's deterrence strategy will be difficult to uphold because the decision process for authorizing a defensive response action following a substantial cyber attack would undoubtedly be untimely, cumbersome, and filled with uncertainty (Wilson, 2007a; Wingfield, 2006).

Chapter 1 serves as an overview for this phenomenological study and includes the background of the problem, the problem statement, the purpose of the study, the significance and nature of the study, a research question, the theoretical framework, definition of key terms, assumptions, limitations, and delimitations. Compensatory (Bueno de Mesquita, 1981, 1984; Meernik, 1994; Ostrom & Job, 1986; Simon, 1959; Steinbruner, 1974; von Neumann & Morgenstern, 1944) and noncompensatory (DeRouen & Sprecher, 2004; Mintz, 1993, 1995, 2004, 2005) decision theories, complexity theory (Anderson, 1999; Hayek, 1964; Holland & Miller, 1991), cyberpower theory (Jordan, 1999; Kramer, Starr, Wentz, Zimet, & Kuehl, 2007), and cyber deterrence theory (Chesser, 2007; Keyes, Simens, Kurtz, & York, 1997; Kugler, 2009) form the research study's theoretical framework. Chapter 1 is concluded with a summary including how the study will add to the body of knowledge of research literature regarding the central phenomenon of decision-making uncertainty with implications for leaders and practitioners in the area of cyber warfare.

Background of the Problem

In a *Tribune* column on nuclear weapons, Orwell (1945) wrote, "The history of civilization is largely the history of weapons" (p. 289). Orwell's observation correlated

societal repression and the rise of tyranny with the cost and availability of weapons (Kampmark, 2007). Essentially, when weapons are inexpensive and available, the “common people” have the opportunity to keep despotism in check. In cyberspace, an individual can control millions of computers (e.g., botnets) as an extremely low cost weapon with catastrophic capability. Therefore, an Orwellian transfer of power to the *common people* is indeed possible (Kampmark, 2007). Through cyberspace, a powerful warfare domain is available to ordinary people with global access to critical infrastructures and information technologies using an inexpensive computer, readily available malicious software tools, and a simple Internet connection.

The end of World War II culminated with the dropping of the first two nuclear devices on Hiroshima and Nagasaki, which spawned the beginning of the nuclear age and the need to deter the devastating effects associated with weapons of mass destruction (WMD). Nearly overnight, the dawning of the nuclear age abruptly reshaped the conventional warfare paradigm honed over the millennia in the minds of strategic military theorists. General Vandenberg (1949) said that a victory in war ceases at its inception and in order to eliminate military deterrence activities, international amity and solidarity must be guaranteed and sustainable.

Two decades after Gibson (1984) coined and described the term “cyberspace” in the science fiction novel, *Neuromancer*, the Department of Defense (DoD) defined cyberspace as the “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (England, 2008a, p. 1). Unlike physical domains (i.e., land, sea, air, space),

cyberspace is a manmade construct that allows global connectivity, virtual existence, and social interaction at speeds approaching that of light. As with all domains, the DoD conducts cyber warfare as an instrument of national power by providing the president with options to enforce responsible behavior, promote democracy, and ensure national security in cyberspace (Pace, 2006a).

Without peacekeeping certainty, the United States is compelled to defend the global populace using nuclear deterrence (Wolk, 1976). With this fundamental premise in mind, the United States has executed an effective strategic deterrence policy since the beginning of the Cold War (Ayson, 2000). However, the effectiveness of classical deterrence is a function of several underlying decision-making and capability assumptions that do not necessarily hold for cyber warfare (Kugler, 2009).

The central idea of deterrence, according to General Cartwright, General Pace, and Secretary Rumsfeld (2006), is to “decisively influence the adversary’s decision-making calculus in order to prevent hostile actions against U.S. vital interests” (p. 5). The primary methods of accomplishing this objective is through denying benefits, imposing costs, and encouraging adversarial restraint (Cartwright et al., 2006). For deterrence to be successful, Kunsman and Lawson (2001) asserted actors must reason, decide, and act rationally with a shared, communal understanding of key values and beliefs. In addition, Schelling’s (1960, 2005) notion of *reciprocal vulnerability* and Schlesinger’s (1976, 1993) spectrum of *credible response capabilities* improve an effective deterrence policy. These fundamental concepts are more complex and immature when developing an enduring cyber deterrence policy (Kugler, 2009; Taipale, 2009).

To begin understanding the uncertainty associated with making the decision to use force following a cyber attack, the decision-maker should consider important similarities and contradictions to traditional warfighting principles. Many leaders, according to McConnell, former Director of National Intelligence, are unaware of the risks that cyber weapons and cyber warfare pose to their organizations (Coleman, 2008a). Specifically, less than 5% of private sector organizations factor cyber attacks and computer viruses into their operational continuity plans (Coleman, 2008a). Even with heightened awareness, leaders should realize that cyber attacks occur at extraordinary speeds relative to traditional warfare. Wilson (2003) warned, “Cyber warfare enables attacks from anywhere in the globe at lightning speed” (p. CRS-29). Therefore, detection and response systems should have automatic features to enhance decision-making.

According to Wilson (2007a), a cyber attack can automatically activate millions of computers worldwide capable of transmitting malicious code and denial of service requests targeted at specific critical computer network servers throughout the Internet. In response to a Congressional question regarding if a cyber attack has the “potential to cause cataclysmic harm if conducted against the United States on a large scale,” the Vice Chairman of the Joint Chiefs of Staff (VCJCS), General Cartwright (Report to Congress, 2007) said:

I don’t think the United States has gotten its head around the issue yet, but I think that we should start to consider that regret factors associated with a cyber attack could, in fact, be in the magnitude of a *weapon of mass destruction*. (p. 96)

Therefore, the scalability and invasiveness of cyber weapons, which are capable of being employed on a global scale, should be treated as a substantial threat to national security.

Unlike traditional warfare considerations, the low cost of entry into the cyber warfare domain allows the range of hostile actors to be geographically and motivationally vast. In cyberspace, Kugler (2009) suggested the three types of adversaries (near-peer rivals, middle-sized rogue countries, and terrorist groups) likely to be encountered bring unique psychologies, motives, attitudes, and agendas to this new virtual battlefield. Kugler added that these rapidly emerging opponents have vastly different perceptions of the U.S. leadership's propensity to demonstrate the will, resolve, and risk-taking courage when responding to cyber attacks in the midst of substantial uncertainty.

Kugler (2009) advised that the strategic context of an encounter in cyberspace could be markedly different from the traditional warfare paradigm. Specifically, potential cyber adversaries are not likely to be traditional nation state actors led by a predictable strategic calculus. On the contrary, cyber attacks will most probably originate from "cyber insurgents" or terrorist networks with different priorities and tolerances for risk, making attribution and the decision process to respond extremely challenging (Thomas, 2006).

The primary challenge of cyber warfare is the attribution of the attack (Gourley, 2008). Serving as a foundational assumption of classical deterrence theory and policy, attribution is the ability to detect the source of an attack and assign credit to a specific adversary with a satisfactory level of certainty (Kugler, 2009; Phillips, 2007; Wheeler & Larsen, 2007). While noting that the accurate and timely identification of the attacker after a computer network attack (CNA) is the most ambiguous and difficult hurdle to overcome, Wilson (2007b) suggested this uncertainty dramatically affects response action decisions (p. CRS-12).

The attribution problem is arguably the single largest factor that differentiates attacks in cyberspace from attacks in other physical domains. To this point, Cartwright et al. (2006) highlighted the immediate need for improving the technical capabilities to support attribution following attacks on computer network systems. When attribution challenges combine with the immaturity of cyber warfare doctrine, warfighters face immense decision-making uncertainty in determining the appropriate response action (Kugler, 2009).

An enduring feature of cyber warfare is likely to be “uncertainty regarding important factors that influence . . . decision-making calculations” (Cartwright et al., 2006, p. 16). Such uncertainties include the identities of key decision-makers, their roles, and the variables considered important when making decisions (Cartwright et al., 2006). Furthermore, the specific uncertainties encountered when considering the proper response action to take following a cyber attack vary from adversary to adversary.

For example, the uncertainty of determining the appropriate response following a cyber attack by a networked non-state actor would most likely be different from the variables that leaders should consider following an attack by a sovereign nation state (Cartwright et al., 2006). Accordingly, decision-makers should plan and conduct cyber warfare in ways that consider such uncertainty factors. Therefore, a more comprehensive understanding of the decision-making uncertainties following a cyber attack is necessary to improve the existing rules of engagement and support the inherent right of self-defense (Peng, Wingfield, et al., 2006).

The fundamental idea of self-defense is founded on the traditionally valid assumption that decision-makers can recognize and decide how to respond following an

attack against the nation's sovereignty (Frank, 1975; Krulak, 1997; Meernik, 1994).

However, this defensive response action assumption does not necessarily hold when adversaries conduct attacks in cyberspace where considerable uncertainty exists (Kugler, 2009; Michael, Wingfield, & Wijesekera, 2003). Nation state leaders demonstrated this uncertainty during the large-scale cyber attacks that occurred against the countries of Estonia and Georgia where command and control, financial, and government networks were inundated by denial of service attacks (Grant, 2007; Nizza, 2008; Wilson, 2007b). In both cases, Estonian and Georgian leaders were unsure of the legal or internationally accepted response to take even after the event was attributed to Russian hackers by their intelligence sources (Coleman, 2008b; Gorman, 2008; Wilson, 2007b).

U.S. information systems are also susceptible to cyber attacks (Reid, 2007). To quantify this assertion, the Pentagon detected over “79,000 attempted cyber attacks in 2005 with approximately 1,300 successful including the penetration of computer systems linked to the Army’s 101st and 82nd Airborne Divisions and the 4th Infantry Division” (Reid, 2007, para. 7). In the same year, Reid (2007) highlighted that cyber attacks against U.S. State Department networks all over the world took hundreds of computers offline for months. In June 2007, a cyber attack took more than 1,500 DoD computers offline requiring days to recover (Peppler, 2007). Following this event, Defense Secretary Gates (2007) said, “The Pentagon sees hundreds of attacks a day from a variety of threats” (para. 2). Peppler (2007) added, “The nature of the threat is large and diverse, and includes recreational hackers, self-styled cyber-vigilantes, various groups with nationalistic or ideological agendas, transnational actors and nation-states” (para. 8).

Statement of the Problem

The general problem is that sovereign nations cannot effectively defend their information systems against cyber attacks because of inadequate international laws and outdated treaties created primarily for making conventional warfare decisions (Coleman, 2008b; Gorman, 2008; Wilson, 2007b). The specific problem is the extent of decision-making uncertainty that senior military leaders experience following a cyber attack prevents the timely and effective determination of the appropriate response, including the use of force (Michael et al., 2003; Moffat, 2003; Owens, Dam, & Lin, 2009; Peng, Wingfield, et al., 2006). Historically, senior military leaders have been effective at making complex decisions regarding the appropriate response following traditional kinetic attacks as evidenced during numerous successful military operations (Elsea, 2006; Meernik, 1994; Waterman, 1997). However, according to Tubbs, Luzwick, and Sharp (2002), the same level of decision-making certainty has not been demonstrated when determining the appropriate response following a cyber attack.

Addressing this problem, Michael et al. (2003) asserted many factors adversely influence the ability to make effective cyber warfare decisions. Specifically, Michael et al. suggested that in order to determine the necessary response action to cyber attacks with the appropriate use of force, the “gray area” of uncertainty must be reduced using a systematic, regimented, and analytical approach. Waters, Ball, and Dudgeon (2008) found, “Commanders at all levels will continue to deal with uncertainty or the ‘fog of war’ due to a lack of complete and accurate information regarding cyber warfare” (p. 86). Complex factors combine to create much uncertainty concerning who conducted the attack and where the attack originated (Waters et al., 2008). The uncertainty after a

computer network attack, such as the accurate and timely identification of the attacker, “may affect decisions about how and against whom, or even whether or not, to retaliate” (Wilson, 2007b, p. CRS-12).

A qualitative, phenomenological study is appropriate for developing a better understanding of the decision-making uncertainty experienced by leaders who make difficult warfare decisions such as when to use force following a cyber attack (Cohen, Etner, & Jeleva, 2008; Creswell, 2005; Dane & Pratt, 2007). The challenges associated with making timely defense response decisions following cyber attacks adversely affect the ability for sovereign nations to execute their inherent right of self-defense (Dinstein, 2002; Robertson, 2002). Therefore, the general population group of this study is comprised of nation state leaders (e.g., Presidents, Secretaries, and Ministers of Defense) responsible for making strategic response decisions following cyber attacks.

Purpose of the Study

The purpose of this qualitative, phenomenological research study was to explore the decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack. A qualitative research method is used when exploring meaning or discovering a central phenomenon (Creswell, 2005; Donalek, 2004). Moreover, Schwandt (2002) suggested qualitative methods provide the best opportunity to obtain a more detailed understanding of the authentic and perceived meaning associated with personal experience. A qualitative, phenomenological research design is appropriate for examining the essence of complex experiential perceptions too difficult to observe or measure through statistical means (van Manen, 1990; Wilding & Whiteford, 2005). Furthermore, this study addressed an apparent deficiency in the

literature regarding the decision-making uncertainty experienced by leaders when determining the proper military response to a cyber attack (Holstein & Gubrium, 1994; Owens et al., 2009; Tubbs et al., 2002).

Phenomenological research designs are most effective at exposing, describing, and developing individual experiences and perceptions based on the participants' insights and expertise (Moustakas, 1994; van Manen, 1990). The research design for this qualitative, phenomenological study used interviews with senior military officers to explore and identify key themes that emerged from their perceptions of the decision-making process following a cyber attack (Groenewald, 2004; Kvale, 1996; Moustakas, 1994). Phenomenological research designs are particularly effective when exploring decision-making opportunities experienced by the participants (Donalek, 2004; Goulding, 2005; Mitroff & Sagasti, 1973; Starks & Trinidad, 2007). Given the role and responsibility of the DoD to protect U.S. information systems against cyber attacks, the specific population group of this study was senior military officers who make cyber warfare decisions as members of the Joint Staff at the Pentagon in Washington, DC.

Significance of the Study

This research study showed insights through lived experiences from senior military officers who make cyber warfare decisions. Research significance included advancing the body of knowledge of cyber warfare and making decisions under conditions of uncertainty within complex environments. In addition, this study was designed to contribute to DoD leaders' understanding about the decisional challenges associated with considering the use of force following a cyber attack. Because an ever-

growing number of cyber attacks are occurring globally, this study may have significance for military leaders and decision-makers worldwide (Vamosi, 2007).

Consistent with the review of the literature presented in chapter 2, the technical and legal communities have conducted substantial research on cyber attacks and their implications (Wilson, 2007a, 2007b; Wingfield, 2006). Saunders and Levis (2007) noted that denial of service attacks, malicious code, and other threats to computer network systems are technically well understood. Furthermore, Silver (2002), building on Sharp's (1999) work, showed that a nation state's response action, including the use of force, is a legal means of exercising the inherent right of self-defense under international law. In addition, considerable research is evident on presidential decision-making processes to use force during traditional warfare (DeRouen, 2000; Meernik, 1994; Mintz, 2004; Ostrom & Job, 1986). However, the literature review indicated research associated with making cyber warfare decisions is lacking.

Due to the complexity of identifying and preventing cyber attacks, Saunders and Levis (2007) recognized an essential need to conduct a thorough examination through formal research in order to understand the decision-making process of countering cyber threats and vulnerabilities. Wilson (2007b) noted that research studies have not adequately addressed the differences between the inherent uncertainties associated with the decision-making processes for considering the use of force following a cyber attack compared to an equivalent kinetic attack. Furthermore, Phister, Fayette, and Krzysiak (2005) remarked, "Basic research that connects decision-making behaviors (desired political-military outcomes at the operational and strategic levels) to specific physical effects (operations and military actions) is necessary to understand how uncertainty

management and decision-making theory” (p. 11) apply when conducting cyber warfare. This research study’s results are expected to make a substantial contribution to the literature regarding cyber warfare decision-making uncertainty.

Significance of the Study to Leadership

According to Saunders and Levis (2007), “Senior leadership across the U.S. government need to work toward a common understanding and appreciation of the critical need to coordinate and develop clear offensive and defensive policy for making operational decisions within the cyber domain” (p. 4). Without an understanding of the uncertainty associated with cyber warfare decisions, the United States could easily succumb to the same level of indecisiveness observed during the Estonia and Georgia cyber attacks (Coleman, 2007; Gorman, 2008). Therefore, visionary leadership and a national research agenda are necessary components for developing sound decision-making processes considering the complexities of the cyber domain (Saunders & Levis, 2007).

By gaining a better understanding of the uncertainties associated with the decision-making processes following a cyber attack, the military readiness of the Joint Staff is anticipated to be enhanced. In addition, this study may be important to National Security Council (NSC) leaders entrusted to implement a legitimate and credible cyber deterrence policy designed to dissuade cyber attacks through the ability to make use of force decisions with confidence and certainty (Kugler, 2009). Furthermore, combatant commanders require robust rules of engagement that empower effective and timely response decisions to cyber attacks (Mathers, 2007). Therefore, this research study may

be important for military leaders and national level decision-makers who make warfare decisions.

Nature of the Study

This qualitative, phenomenological research study was used to explore the central phenomenon of decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack. A qualitative research method is used when exploring meaning or discovering understanding of a central phenomenon (Creswell, 2007; Neuman, 2005). Phenomenological research is useful in gaining an understanding of an individual's subjective perceptions and interpretation of a phenomenon based on lived experiences (Moustakas, 1994). Mertens (2005) suggested that the difference between phenomenological research and other qualitative research designs is the individual's personal experiences are the focal point of the investigation. The intent is to understand and describe a phenomenon using the participant's viewpoint (van Manen, 1990).

Interpretive and phenomenological methods were combined in this study through a series of interviews designed to allow the research participants to reflect on and construct meaning based on their own decision-making uncertainty experiences. As the participant's experiences and perceptions emerged into consciousness through the interview process, key themes and patterns were used to develop a narrative of data by examining and exploring the responses using the modified van Kaam (1959) method (Moustakas, 1994). The modified van Kaam method was the data analysis process used for this qualitative research study because this methodology incorporates an appropriate

and systematic approach for organizing, analyzing, and synthesizing the collected data (Moustakas, 1994).

This research study was designed to explore the lived experiences of senior military officers who served for the Chairman of the Joint Chiefs of Staff (CJCS) in cyber divisions at the Pentagon in Washington, DC. Specifically, by reflecting on and synthesizing the essence of the participants' responses through phenomenological research methods, the goal of this study was to gain a better understanding of the uncertainty senior military officers experience when making response decisions following a cyber attack. Senior military officers were defined as Army, Navy, Air Force, and Marine Corps officers in pay grades O5 (Lieutenant Colonels or Commanders) and above. Cyber divisions were defined as Joint Staff divisions where cyber warfare analysis, risk assessment, and strategic decision-making occur within the following directorates: J2 (Intelligence), J3 (Operations), J5 (Strategic Plans and Policy), J6 (Computers and Communications), J7 (Operational Plans and Doctrine), J8 (Force Structure and Resources), and Joint Staff Legal.

Appropriateness of the research method. Qualitative research methods are used to explore phenomena or experiences with the goal of better understanding the contextual meaning of the collected data (Creswell, 2007). Neuman (2005) added that qualitative research methods are best when seeking to understand real-world phenomena that occur in a natural setting. According to Blum and Muirhead (2005), qualitative research methods should be used “to describe and interpret data . . . when the problem is focused on what is or was occurring, inquiring about processes, views, and detailed information . . . where no preconceived models exist” (p. 8). Because the goal of this research study

was to capture the essence of human experiences as portrayed by the participants, qualitative research methods were more appropriate than quantitative methods when seeking to gain a deeper understanding of multiple perceived realities (Creswell, 2007; Leedy & Ormrod, 2010; Lincoln & Guba, 1985).

Qualitative research methods met the goals of this study based on the following considerations. The primary research objective for this study was to understand the lived experiences and perceptions of senior military officers following a cyber attack. Qualitative methods are designed to understand individuals and events in natural settings (Holosko, 2006; Leedy & Ormrod, 2010). Qualitative research is an *inductive* process that explores a problem by proceeding from “a general point of view to a specific conclusion” (Holosko, 2006, p. 13). This study’s logical orientation followed the inductive process by exploring the separate experiences and perceptions of individual participants with the goal of discovering common themes and constructing a composite description of the decision-making uncertainty phenomenon. Qualitative research is the preferred method when studying leadership phenomena such as decision-making uncertainty (Bryman, Bresnen, Beardsworth, & Keil, 1988; Conger, 1998; Yukl, 1989).

The epistemological perspective should be considered when determining the research methodology (Holosko, 2006). Qualitative research is primarily interpretive whereas quantitative research is mainly positivistic (Bryman, 1984; Dobrovolny & Fuentes, 2008; Holosko, 2006). This qualitative study was part of the interpretive paradigm (seeking to understand) with the objective of understanding the decision-making experiences as described by senior military officers. For qualitative methods, researchers must immerse themselves into the natural setting and become an integral part

of the participants' experiential perspective (Holosko, 2006; Ospina, 2004). The nascent and complex nature of the phenomenon under investigation in this study necessitated the collection of highly descriptive and contextual narratives in order to understand the lived experiences and perceptions of a limited number of participants.

The availability and use of theory and theoretical frameworks should be evaluated when selecting the research methodology (Blum & Muirhead, 2005; Holosko, 2006). In qualitative methods, researchers need not use specific theories to frame their study initially (Creswell, 2007; Holosko, 2006). The data collected in quantitative studies are designed to verify or refute the base theory from which the hypotheses were formulated. For this research study, the review of the literature indicated no single theory exists for the phenomenon under study (Bartholomees, 2008; Czerwinski, 1998; DeRouen, 2000; Hansson, 2005; Schultz, 1997; Yukl, 1989). Therefore, qualitative methods were more appropriate for studying a phenomenon of this complexity (Eldabi, Irani, Paul, & Love, 2002).

Last, the researcher's role during the data collection process should be considered when determining the proper research method (Creswell, 2007; Holosko, 2006; Smith, 1983). When conducting qualitative research, the "researcher is the instrument" (Patton, 2002, p. 14). Therefore, the researcher is actively engaged and immersed in the natural environment under study while data are collected from participants (Dobrovolny & Fuentes; 2008; Holosko, 2006). For this study, the goal was to create a participant-observer role using qualitative methods in which lived experiences and perceptions were explored using "induction to analyze collected data (e.g., code interview transcripts, identify themes and patterns)" (Dobrovolny & Fuentes; 2008, p. 9).

Quantitative methods were inappropriate for this research study for several reasons. First, the number of individuals with considerable cyber warfare decision-making experience was extremely limited. Therefore, the sample would not have been statistically significant and the results would have been prone to large standard errors (Creswell, 2009). Second, the number of cyber attacks substantial enough to consider the use of force is also limited. Consequently, insufficient data would have been available to analyze research variables such as the Schmitt (1999) cyber attack parameters (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility) for trends, correlations, and hypotheses testing.

Third, quantitative methods would not have permitted the rich open-ended discussion capable of stimulating the individual lived experiences and perceptions of senior military officers who make cyber warfare decisions (Creswell, 2007, 2009; Hycner, 1985; Kvale, 1996; Moustakas, 1994). In general, the researcher conducting a quantitative study has a passive, separated, and often detached role from the research subjects (Bryman, 1984; Dobrovolsky & Fuentes; 2008; Holosko, 2006). Therefore, the resulting outcome of quantitative research is an impersonal, objective report of the research findings displayed using numerical and graphical methods (Dobrovolsky & Fuentes; 2008). Finally, the nature of the research question, the complexity of the central phenomenon, the lack of a coherent theoretical framework, the paucity of supporting literature, and the desire to explore the lived experiences and perceptions of the participants, made quantitative methods inappropriate for this research study (Creswell, 2009; Dobrovolsky & Fuentes; 2008; Leedy & Ormrod, 2010).

Appropriateness of the research design. A phenomenological design was used for this qualitative research study to explore the lived experiences and perceptions of senior military officers following a cyber attack. Phenomenology is the study of lived experiences as described by individuals who experienced the phenomena (Burrell & Morgan, 1979; Husserl & Welton, 1999; Moustakas, 1994; Schutz, 1967). Building on Kant (1764), Hegel (1807), and Brentano's (1874) early philosophical work, Husserl (1859-1938), a German mathematician and logician, is attributed with developing the conceptual framework of transcendental phenomenology (Dowling, 2007; Moustakas, 1994; Priest, 2002; van Manen, 1990). Husserl's objective was "to discover the nature, goals, and methods of philosophical inquiry" (Priest, 2002, p. 51).

Phenomenology was the most appropriate qualitative research design compared to other research designs considered for this study. Transcendental phenomenology, as a method of inquiry, is a structured process of understanding a central phenomenon as described by the participants (Moustakas, 1994). The objective of this study was to understand the experiential essence of cyber warfare decision-making uncertainty as described by the senior military officers. Therefore, the research goals of this study were achieved by using *phenomenological reduction* to facilitate the transcendence and description of the participants' experiences (Priest, 2002).

According to Moustakas (1994), Husserl embraced Bertano's notion of *intentionality* as the "fundamental concept for understanding and classifying conscious acts and experiential mental practices" (Dowling, 2007, p. 132). Husserl also recognized *intuition* as a key concept of transcendental phenomenology (Moustakas, 1994). In this context, Husserl adopted Descartes' (1644/1983) interpretation of intuition as "an inborn

talent directed toward producing solid and true judgments concerning everything that presents itself” (p. 22). Therefore, the essence of Husserl’s theory is intentionality and intuition manifested through the ability to make judgments as knowledge emerges to consciousness (Husserl, 1931; Moustakas, 1994).

Phenomenological research designs are particularly well suited for exploring decision-making experiences (Anderson & Eppard, 1998; Donalek, 2004; Karlsson, 1992; Starks & Trinidad, 2007). This assertion is based on the similarities between the epistemological principles fundamental to phenomenology and decision-making (Karlsson, 1992; Mitroff & Sagasti, 1973). Specifically, phenomenology is founded on the premise that experience is the primary source of knowledge through the lens of intentionality and intuition (Husserl, 1931; Moustakas, 1994; Priest, 2002). Similarly, Pace (2006b) wrote, “Effective decision-making combines judgment and intuition acquired from experience, training, study, and creative thinking. Commanders visualize the situation and make sound and timely decisions” (p. III-2). Decision-making is a complex process occurring along a spectrum of certainty in which probability distributions, experience, intuition, rationality, risk acceptance, beliefs, and values factor into the decision calculus (Bennet & Bennet, 2008; Böhm & Brun, 2008; Vowell, 2004).

Giorgi (2006) found that many variations of Husserlian phenomenology exist among the more prominent phenomenological research psychologists. Specifically, Giorgi conducted an analysis of the phenomenological designs published by Colaizzi (1973), Giorgi (1985), Hycner (1985), Karlsson (1993), Moustakas (1994), and van Manen (1990). Although several differences were found between each design using phenomenological criteria, Giorgi asserted the key similarities were founded on

understanding the “phenomenon being experienced and not . . . the particular individual who is experiencing the phenomenon” (p. 318). For this study, the research design was primarily centered on Moustakas’ interpretation of Husserl’s phenomenology including the modified van Kaam (1959) method of data analysis.

Other qualitative research designs considered. In addition to phenomenology, several other qualitative research designs were considered for this research study. Specifically, ethnography, case study, Delphi technique, and grounded theory were evaluated for appropriateness. Although these research designs have characteristics well suited to particular qualitative studies, none was capable of meeting this study’s research goals better than phenomenology. Therefore, these designs were rejected based on the following considerations.

Ethnography. An ethnographic design was not appropriate for this research study. First, observing the decision-making uncertainty that senior military officers experience following a cyber attack is not logistically feasible. Because cyber attacks are discrete and unpredictable events that occur without notice, conducting direct observation fieldwork was not realistic. Furthermore, the decisional process following a cyber attack occurs in different locations within the Pentagon based on the attack’s characteristics and effects. Therefore, the ability to predict the observation location accurately would be highly unlikely. Last, the purpose of this study was to gain an understanding of the individual lived experiences and perceptions of senior military officers following a cyber attack without preconceived causality. Therefore, an ethnographic inquiry would have inappropriately indicated the decisional experiences were associated with a particular belief system, social setting, or cultural interaction.

Case study. The case study design was inappropriate for this research study for several reasons. Schramm (1971) wrote, “The essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a *decision* or set of decisions: why they were taken, how they were implemented, and with what result” (p. 21). However, this study was used to explore decision-making uncertainty following a cyber attack by understanding the lived experiences and perceptions of senior military officers versus why or how particular decisions were made to achieve a particular end state. Although data were collected in this study using individual interviews, key themes emerged common among senior military officers, as a collective group of the Joint Staff. The case study design would have been limited in extracting these communal behaviors and experiences (Stake, 1995; Yin, 2009).

Because the specific details and analysis parameters associated with actual cyber attack cases contain highly classified information, a case study’s findings would not have been releasable or publishable (Wilson, 2007b). Furthermore, this study’s goal was to improve the understanding of the decisional uncertainty experienced by senior military officers following cyber attacks of various severities and intensities. Therefore, using the case study approach to research a particular, unclassified cyber attack would have unnecessarily limited the scope of this understanding.

Delphi technique. Several important considerations made the Delphi technique inappropriate for this research study. First, the purpose of this study was to explore the lived experiences and perceptions of senior military officers and not to develop a decision or create a new policy about cyber warfare. Second, senior military officers comprised the population for this study. Even though the officers are experts in cyber warfighting

doctrine, they were not necessarily experts in decision theory, uncertainty theory, or the technical aspects of a cyber attack (Linstone & Turoff, 1975). Therefore, assembling a group of *experts* based on meaningful criteria and suitable for answering complex questions regarding decision-making uncertainty would not have been achievable or defensible using the desired population (Rowe & Wright, 1999). Finally, existing policy prohibits Joint Staff members from developing a decision or policy for unofficial purposes that could be construed to reflect the opinion of the Joint Staff, the DoD, or a particular military department (D. A. Armstrong, personal communication, January 13, 2009).

Grounded theory. A grounded theory design was inappropriate for this research study. First, the purpose of this study was to explore the lived experiences and perceptions of senior military officers following a cyber attack and not to develop a process theory that explains actions or activities associated with the central phenomenon. Second, grounded theory as a research design “. . . was developed for, and is particularly suited to, the study of behavior” (Goulding, 1998, p. 56). However, the key themes and invariant constituents that emerged from exploring the lived experiences and perceptions associated with decision-making uncertainty were not necessarily caused by the participants’ behavior. Specifically, decision-making uncertainty in cyber warfare is a function of many other factors such as social, cultural, cognitive, technical, and ethical aspects (Aiello, 2008; Borgmann, 2004; Pace, 2006a; Rowe, 2007). Using a phenomenological approach allowed these areas to be explored fully without this design limitation.

The third concern with a grounded theory approach was associated with the coding procedure. Strauss and Corbin (1990) added an additional coding step to the grounded theory comparative analysis procedure originally developed by Glaser and Strauss (1967). This step, known as *axial coding*, was placed between the initial *open* and final *theoretical* coding steps as a means of facilitating the process. During the axial coding process, researchers place all open-coded data into six predetermined categories: causal conditions, phenomena, context, intervening conditions, actions/interaction strategies, and consequences (Strauss & Corbin, 1990). Unfortunately, critics of the axial coding process assert the intermediate step is unnecessarily restrictive and artificially limits the exploration to the six predetermined categories of the Strauss and Corbin paradigm model (Glaser, 1992; Hall & Callery, 2001; Kendall, 1999).

The last concern with grounded theory was associated with the data collection requirements to reach theoretical saturation. A substantial number of participants are required for grounded theory research in comparison to other qualitative research designs (Charmaz, 2006; Creswell, 2005; Goulding, 1998, 2005). Because the number of senior military officers with credible cyber warfare experience assigned to the Joint Staff was limited to approximately 30, the potential existed that the number of willing participants would have been exhausted prior to a new theory emerging from the collected data. Therefore, considering the four concerns presented above, grounded theory research was inappropriate for this research study.

Research Question

The decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack was explored in this qualitative,

phenomenological research study. Therefore, gaining a better understanding of the decision-making uncertainties encountered by senior military officers following a cyber attack through their perceptions and lived experiences was the focus of this study.

Moustakas (1994) stated, “The method of reflection that occurs throughout the phenomenological approach provides a logical, systematic, and coherent resource for carrying out the analysis and synthesis needed to arrive at essential descriptions of experience” (p. 47). To explore the identified phenomenon while facilitating the reflection of the experiential descriptions, this study was guided by the following research question: *How do senior military officers perceive and describe the lived experience of decision-making uncertainty when determining the appropriate response to a cyber attack?*

The research question was open-ended and non-directional in order to obtain the lived experiences of the research participants in an environment that minimized researcher bias and encouraged the identification of alternative perspectives. Leedy and Ormrod (2010) noted, “Qualitative researchers construct interpretive narratives from their data and try to capture the complexity of the phenomenon under study” (p. 103). Creswell (2005) found this approach often exposes additional questions thus forming a basis for future research. Care was taken during the interview process to establish an atmosphere conducive for the participants to remember and express their thoughts, ideas, and perceptions freely using neutral prompts to ensure their experiences were described fully.

Theoretical Framework

The theoretical framework for this research study was based on Drucker's (2007) effective decision-making model in conjunction with compensatory (e.g., expected utility and cybernetic; Bueno de Mesquita, 1981, 1984; Meernik, 1994; Ostrom & Job, 1986; Simon, 1959; Steinbruner, 1974; von Neumann & Morgenstern, 1944) and noncompensatory (e.g., poliheuristic; DeRouen & Sprecher, 2004; Mintz, 1993, 2004, 2005) decision theories, complexity theory (Anderson, 1999; Hayek, 1964; Holland & Miller, 1991), cyberpower theory (Jordan, 1999; Kramer et al., 2007), and cyber deterrence theory (Chesser, 2007; Keyes et al., 1997; Kugler, 2009). Decision theory was used to form the fundamental rules and principles required to rationalize the research problem into a generic statement using appropriate and applicable specifications (Drucker, 2007). The general problem statement was delimited using complexity theory to establish the governing boundary conditions (Holland & Miller, 1991; Suh, 1999, 2005). Cyberpower theory was used to describe how cyber capabilities could be leveraged as an instrument of national power (Kramer et al., 2007). Building on cyberpower theory, the set of potential actions the decision-maker should consider to dissuade, deter, or prevent a cyber attack was refined using cyber deterrence theory (Chesser, 2007; Kugler, 2009).

Compensatory decision-making models. Rational, compensatory models predict that leaders choose an “alternative that maximizes utility on the basis of a holistic comparison process as suggested by the expected utility model, or selecting an alternative that ‘satisfices’ a certain criterion as predicted by the cybernetic model” (Mintz, 2004, p. 595). Bueno de Mesquita and Lalman (1990) suggested, “Nations are led by rational,

forward-looking, expected-utility-maximizing leaders who make [use of force] decisions in a holistic and compensatory (additive) fashion” (p. 751). The use of force decisions these leaders make are derived from the strategic values associated with alternative outcomes and an estimate of how adversaries will respond based on their belief systems (Bueno de Mesquita & Lalman, 1990).

Decision-makers assess the advantages (benefits) and disadvantages (costs) related to each alternative to attain “the largest net gain (expected utility) at an acceptable level of risk” (Bueno de Mesquita, 1984, p. 228). Although expected utility theory is “the leading decision paradigm in international relations” (p. 3), Mintz (2004) argued the theory has several limitations. Specifically, cognitive psychologists and behavioral organization theorists have found analytical decision-making strategies, such as expected utility theory, require “extensive processing time, cognitive effort, concentration, and skills that in many cases are not available, especially under time pressures and rapidly changing conditions [such as cyber warfare]” (Mintz, 1993, p. 596).

Ostrom and Job (1986) developed the cybernetic model in an attempt to explain how individuals make decisions in environments dominated by complexity and uncertainty. This model extends well to the decision process to use force (Waterman, 1997). According to the “bounded rational model, of which the cybernetic satisficing model of decision-making is one type, leaders operate under constraints while searching for an acceptable outcome” (Mintz, 1993, p. 596). The cybernetic model presumes the leader is not able to “monitor and respond to all incoming stimuli from the domestic and international environments; rather decision-making should be viewed as operating in an environment with reduced information-processing capabilities as well as limited

cognitive ability” (Waterman, 1997, p. 8). A cybernetic decision-maker is one who “makes decisions concerning the use of force based on careful examination of a select number of environmental stimuli or variables” (Waterman, 1997, p. 8). Consequently, cybernetic decision processes are “less comprehensive because only a subset of alternatives and dimensions is considered” (Mintz, 1993, p. 596).

Noncompensatory decision-making models. Compensatory models are linear, additive models where “each dimension for a decision alternative is given a value and the dimensions are combined additively to produce an overall value for each alternative” (Mintz, 1993, p. 597). With compensatory models, a “high score on the military or international dimension can ‘compensate’ for a low score on the political variable and vice versa because the leader makes a decision to use force based on the *overall* score” (Mintz, 1993, p. 597). In contrast, noncompensatory models indicate that decisions are based not on a compensatory calculus, but “in a choice situation, if a certain alternative is unacceptable on a given dimension, then a high score on another dimension cannot compensate/counteract for it, and hence the alternative is eliminated” (Mintz, 1993, p. 578). Therefore, Mintz (2004) proposed, “Decisions on the use of force are often made based on the rejection of undesirable alternatives on the basis of one, or at most a few, criteria” (Mintz, 2004, p. 595).

Noncompensatory models capture the non-holistic nature of decision-making by focusing on a limited set of alternatives and dimensions. Instead of assessing all alternatives using a weighted summative analytical process, the decision-maker “adopts heuristic decision rules that do not require detailed and complicated comparisons of relevant alternatives, and adopts or rejects undesirable alternatives on the basis of one or

a few criteria” (Mintz, 1993, p. 579). Whereas the expected utility and cybernetic use of force models are alternative-based, noncompensatory models are dimensional or attribute based (Mintz, 1993). In this context, a dimension is an organizing theme for related information and variables (Ostrom & Job, 1986). In the compensatory linear model, the values of dimensions are summed as utility scores to form an alternative. In contrast, the value of a *critical* dimension is evaluated against a threshold level in the noncompensatory model. If a critical dimension’s expected value is less than a predetermined threshold, the respective alternative is removed from further consideration (Mintz, 1993).

Poliheuristic theory “bridges the gap between cognitive and rational theories of decision-making” (Mintz, 2004, p. 3). Poliheuristic choice theory is based on a two-stage decision process. In the first step, according to DeRouen and Sprecher (2004), alternatives are eliminated by a noncompensatory analysis using simplified heuristics (i.e., cognitive shortcuts). In the second step, the remaining alternatives are evaluated by employing a rational or compensatory means by seeking to minimize risks and maximize benefits (Mintz, 2004). Examples of the noncompensatory heuristics that inform the elimination of options include “political constraints on the use of force” (Mintz, 2004, p. 3). Poliheuristic theory is used to expose the results of the decision-making opportunity by explaining why and how leaders make decisions. According to Mintz (2004), poliheuristic theory has been applied to a myriad of decision-making situations including the use of force (Mintz, 1993), diversionary use of force (DeRouen, 2000; Nincic, 1997), initial crisis reaction (DeRouen & Sprecher, 2004), and the level of force used in a crisis (Redd, 2002).

Complexity theory. Complex phenomena are characterized by abstract patterns resulting from the interactions between numerous variables (Hayek, 1964). Complexity theory is used to describe the characteristics and dynamical behavior of complex adaptive systems using the foundational premises of systems theory, catastrophe theory, and chaos theory (Anderson, 1999; Bertalanffy, 1972; Glenn, 2002; Holland & Miller, 1991).

Bennet and Bennet (2008) suggested the condition and dynamics of nonlinear systems, situations, or organizations could be described with more elements and relationships using complexity theory than employing normal analytical techniques or logical methods alone. When developing a decision strategy to use when considering the appropriate response following a cyber attack, the plan should include boundary conditions, tipping points and butterfly effects, stability patterns, equilibrium factors, regenerative feedback loops, and external perturbations (Bennet & Bennet, 2008).

Cyberpower theory. Jordan (1999) developed a theory of cyberpower based on three interconnected regimes: power from an individual's viewpoint, a social perspective, and the collective imagination. According to Jordan, understanding cyberpower requires a thorough grasp of the theories of power. Therefore, Jordan built a cyberpower theory based on "Max Weber's common sense theory of power as the possession of individuals, Barry Barnes' theory of power as the constituent of social order, and Michel Foucault's analysis of power as domination" (p. 4).

On an individual level, cyberpower is the product of "identity fluidity, the remaking of hierarchy, and spaces made out of information" (Jordan, 1999, p. 5). These three dimensions form a cyberpower framework comprised of "access, privacy, encryption, copyright, and censorship that offers power [in cyberspace] to the individual"

(Jordan, 1999, p. 5). According to Jordan (1999), cyberpower becomes formidable when the individual, social, and cognitive forces coalesce through the interrelation of the three fundamental levels of the virtual social order.

Kramer et al. (2007) developed a cyberpower theory based on a strategic framework to describe, explain, and predict how national leaders should best use cyberpower in support of U.S. national security interests. Kramer et al. defined cyberpower as the “ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power” (p. 4). In this theoretical model, Kramer et al. used a hierarchy of measures of merit (MoMs) to build a layered approach to the cyberpower framework.

Kramer’s et al. (2007) cyberpower model is comprised of three layers visualized in the form of a pyramid. The cyber infrastructure (Layer 1) is characterized by measures of performance (MoPs) such as bandwidth and connectivity per capita (Kramer et al., 2007). The levers of power (Layer 2) are represented by measures of effectiveness (MoEs) such as the achievement of military operational objectives or changes in loss exchange ratios (Kramer et al., 2007). The empowerment of key entities (Layer 3) is described by measures of entity empowerment (MoEEs) such as the extent to which an entity can perform key functions and missions as a function of the capability afforded by cyberpower (Kramer et al., 2007). As an example, cyberpower enables an individual or group to use the nature of cyberspace to shape global events by exerting influence over key decision-making processes (Kramer et al., 2007).

Cyber deterrence theory. In 1959, Brodie defined deterrence as “the prevention from action by fear of the consequences” (p. 34). Based on this definition, historian

Howard (1994-95) postulated a “strategic paradigm based on deterrence, compellence, and reassurance . . . where military power can deter other states from doing something, compel them to do something, or reassure them of a general sense of security” (p. 165). In 1997, Keyes et al. published one of the first noteworthy reports that highlighted the differences between classical deterrence and cyber deterrence. Specifically, Keyes et al. realized, in cyberspace, the United States cannot rely on any advance warning time to dissuade a potential adversary. Furthermore, the United States lacks the technical capabilities and national security policies to take preemptive actions to prevent a cyber attack (Keyes et al., 1997). In this germinal work, Keyes et al. (1997) proposed a three-step process toward building an effective cyber deterrence strategy. First, the president should declare a policy and build international consensus. Second, U.S. government agencies and departments should harden potential targets and impede/deny access to them. Last, the U.S. government should broadly share information, thoroughly conduct analysis of cyber attacks, and issue warning notices concerning discovered threats and vulnerabilities (Keyes et al., 1997).

Building on Keyes’ et al. (1997) concepts, Khalilzad (1999) proposed three basic strategies for defending against cyber warfare: protection, deterrence, and prevention. In Khalilzad’s construct, protection reduces vulnerabilities by increasing resiliency through hardening potential targets, reducing the resultant damage, and improving the capability to recover expeditiously. Deterrence, according to Khalilzad, reduces the motivation for malicious actors to conduct network warfare based on credible retaliatory capabilities. Finally, prevention reduces the capacity and hinders the capability for adversaries to obtain and effectively employ cyber weapons and techniques (Khalilzad, 1999). Before a

cyber deterrence policy can be effective, Khalilzad asserted that a cyber deterrence theory should effectively address the fundamental differences between conventional, nuclear, and cyber warfare.

Kugler (2009) developed a cyber deterrence theory by extending the principles associated with Brodie's (1946, 1959) and Schelling's (1966) classical strategic deterrence theory while accounting for the technical, social, and cognitive distinctions inherent to cyberspace, which were highlighted by Keyes et al. (1997) and Khalilzad (1999). Kugler asserted a "one-size-fits-all approach to [cyber] deterrence will not work because of the multiplicity and diversity of potential adversaries and cyber attacks" (p. 15). Therefore, a cyber deterrence strategy should be "tailored" to treat each category of potential adversary, type of attack, and type of response on its own merits using an ends, ways, and means construct (Kugler, 2009).

Chesser's (2007) deterrence model builds on and generalizes classical decision theory, which is generally comprised of utility and probability theories, to include performance measures and uncertainty theories (Eberbach, 2005). According to Chesser, "Decision makers, policy makers, and commanders at all levels need to understand deterrence theory applicable to the 21st century security environment" (p. 1). Specifically, Chesser advised that leaders require a deterrence typology to "understand the ways and means to deter a non-nation-state actor while simultaneously retaining the means to deter and compel nation-states" (p. 1). Chesser's theoretical deterrence model is built on a deterrence analysis and planning support environment "embedded in an effects-based paradigm that begins with identifying the deterrent effect the user is seeking" (Chesser, 2007, p. 1).

Definition of Terms

Following are definitions of key terms used in this qualitative, phenomenological study.

Computer Network Attack (CNA). CNA is comprised of “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves” (Sharp, 2006, p. GL-5).

Cyber Attack. “A computer network attack or other malicious activity in cyberspace directed against a nation state that causes an effect, which invokes that state’s inherent right of self-defense” (W. G. Sharp, personal communication, July 25, 2008).

Cyber Warfare. Warfare engaged in cyberspace. The use of force in cyberspace intended to cause intentional harm to people, assets, or economies (Hildreth, 2001; Janczewski & Colarik, 2008).

Cyberspace. Cyberspace is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (England, 2008a, p. 1).

Elements of National Power. The elements of national power are the “response options available to the President of the United States including diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL)” (Josten, 2006, p. 16).

Uncertainty. The indeterminate condition faced by a decision-maker when outcomes will occur with probabilities that cannot be measured or estimated; immeasurable risk (Knight, 1921).

Use of Force. “Physical actions taken by one or more components of the uniformed military Services as part of a deliberate attempt by the national authorities to influence . . . specific behavior of individuals in another nation” (Blechman & Kaplan, 1978, p. 12). Use of force is “a state activity that threatens the territorial integrity or political independence of another state within the meaning of Article 2(4) of the Charter of the United Nations” (Sharp, 1999a, p. 118).

Assumptions

In this study, four assumptions were made related to the phenomenological research design’s reliance on the ability to collect, analyze, and interpret the lived experiences of the participants accurately and reliably (Moustakas, 1994). The first assumption was the participants would be interested and willing to share their perceptions and lived experiences openly, honestly, and completely. Second, the data collection process was assumed to be valid and conducted with due diligence. The third assumption was the analysis tools were accurate and unbiased. Finally, the selected research design of phenomenology was assumed to yield rich and relevant results enabling senior military officers to have a better understanding of their decision-making uncertainty following a cyber attack.

Scope

The scope of this qualitative, phenomenological study focused on senior military officers serving in cyber warfare divisions on the Joint Staff at the Pentagon in Washington, DC. Because the specific sample size for qualitative research methods cannot be predetermined with exact precision, the intent of this study was to interview senior military officers until no new key themes emerge (Groenewald, 2004; Moustakas,

1994; van Manen, 1990). Typically, approximately 20 participants are required to reach thematic saturation in phenomenological research studies (Boyd, 2001; Creswell, 2007; Luborsky & Rubenstein, 1995). Therefore, the number of senior military officers meeting the purposive sampling criteria and available to participate in this research study was adequate. Senior military officers who serve as members on the Joint Staff are screened and assigned specifically based on their superlative military records including warfare decision-making experience (M. D. Johnson, personal communication, June 12, 2009). Face-to-face interviews were used as the method of data collection.

Limitations

Limitations indicate the potential weaknesses of the study outside the control of the researcher (Kornuta & Germaine, 2006) and establish the “boundaries, exceptions, reservations, and qualifications inherent in every study” (Creswell, 1994, p. 110). Three general limitations applied to this study. This phenomenological research study was limited to participants who agree to participate voluntarily, the amount of time available to conduct the study, and the reliability of the research instrument (interview process). In addition, four specific limitations were evident.

First, the research study population was limited to senior military officers with specialized cyber warfare decision-making experience. Second, the research study was limited to participants responsible for cyber attacks against DoD information systems. Third, the researcher’s military warfare experience and perceptual distortions might have introduced unintended limitations (Moustakas, 1994). The final limitation was associated with the interview process including information filtered through the participants’ perceptions with the understanding that not all participants would be equally articulate,

self-reflective, or experienced (Creswell, 2005). By applying epoché (i.e., allowing empathy and connection, not elimination, replacement or substitution of perceived bias) and bracketing (i.e., facilitating recognition of the essence of meaning of the phenomenon under scrutiny), the researcher's bias associated with preconceived notions about decision-making uncertainty was minimized (Bednall, 2006).

Delimitations

Delimitations are the intentional boundaries placed on the study to narrow the scope and to make the study more manageable (Kornuta & Germaine, 2006; Leedy & Ormrod, 2010). Due to the desired level of the participants' decision-making experience for this study, the interviews were confined to senior military officers serving in cyber divisions on the Joint Staff at the Pentagon in Washington, DC. For this study, the senior military officers were Army, Navy, Air Force, and Marine Corps officers in pay grades O5 (Lieutenant Colonels or Commanders) and above. Only cyber attacks against computer systems, networks, and information technology infrastructures that service the Global Information Grid (GIG) and the defense industrial base (DIB) were considered (Motteff & Parfomak, 2004; Pace, 2006a). The content of this research study was restricted to unclassified events, scenarios, tactics, techniques, and procedures.

The generalizability for qualitative studies is limited. Creswell (2009) stated, "The intent of qualitative research is not to generalize findings, but to form a unique interpretation of events" (pp. 158-159). Priest (2002) considered generalizing across populations in different settings to be a weak aspect of qualitative research. Priest emphasized this point was even more germane when participants were selected purposively, as was the case for this study. However, readers might wish to apply the

results of this study based on an understanding of “detailed information regarding participants, selection methods, context, and data generation and analysis methods” (Priest, 2002, p. 60). Specifically, military leaders internationally might find the insights and experiences of their U.S. counterparts particularly useful when supporting national decision-making processes following a large-scale cyber attack.

Summary

Chapter 1 included a description of how the uncertainty associated with making cyber warfare decisions in response to an ever-increasing number of cyber attacks negatively affects warfighting readiness and the ability to implement an effective cyber deterrence policy (Pace, 2006a; Lewis, 2007; Rhodin, 2008; Shachtman, 2008). The uncertainty experienced when making the decision to respond to a cyber attack is not consistent with the decision process maturity following an equivalent kinetic attack (Sharp, 1999a; Michael et al., 2003; Wilson, 2007b). For this research study, a qualitative, phenomenological design was used to explore the central phenomenon of decision-making uncertainty following a cyber attack.

Significance of this study was based on an apparent gap in the research literature regarding the uncertainty associated with making cyber warfare decisions for both senior military officers and national level decision-makers (Phister et al., 2005). Compensatory (Bueno de Mesquita, 1981, 1984; Meernik, 1994; Ostrom & Job, 1986; Steinbruner, 1974) and noncompensatory (DeRouen & Sprecher, 2004; Mintz, 1993, 2004, 2005) decision theories, complexity theory (Anderson, 1999; Hayek, 1964; Holland & Miller, 1991), cyberpower theory (Jordan, 1999; Kramer et al., 2007), and cyber deterrence

theory (Chesser, 2007; Keyes et al., 1997; Kugler, 2009) formed the theoretical foundation of this research study.

In chapter 2, a review of the literature regarding decision-making uncertainty associated with determining the appropriate response following a cyber attack is presented. An explanation of how the literature review was conducted from a strategic perspective is provided. Chapter 2 includes a historic perspective of cyberspace, an overview of cyber warfare, a description of the legal governance structure, and current findings and studies related to the study's theoretical framework.

Chapter 2: Review of the Literature

The U.S. economy and national security are fully dependent on cyberspace (Bush, 2003). Unfortunately, cyberspace is extremely vulnerable to numerous threats from a spectrum of malicious actors who conduct attacks that range from nation state sanctioned computer network operations (CNO) to hackers conducting cyber crime activities. Experts predict cyber attacks will supplement and enable traditional military activities in the near future with physical and cyber targets aligned during hostile operations (Matthews, 2008).

Furthermore, cyber warfare activity will continue to increase due to the “low cost of conducting cyber attacks versus physical attacks, the lack of effective computer network defenses, the plausible deniability the Internet affords, and the lack of ‘cyber rules of engagement’ between nation states” (Ahamad et al., 2008, p. 5). Therefore, understanding how to make warfighting decisions following a cyber attack is vital to national security. The purpose of this qualitative, phenomenological research study was to explore the decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack.

Chapter 2 includes a comprehensive review of the literature on cyberspace, cyber warfare, decision theory, and uncertainty theory from a military perspective using germinal, key, and current findings. The review of the literature begins with a description of the strategy used to conduct the review followed by an accounting of the different types of literature used to support the research study. The review of the literature was based primarily on recent findings within peer reviewed journal articles, technical documents/reports, periodicals, and books, except for historical references that

provide germinal and theoretical evidence related to the research study's central phenomenon. Following a historical overview, details on the research factors designed to provide scope, meaning, and context of the study are provided. Chapter 2 is culminated with conclusions derived from an analysis of the literature review. Following a comprehensive discussion of the limitations and gaps discovered in the research literature, a summary of key points is provided.

Documentation

To gain a deeper understanding of the uncertainty associated with making decisions to use force following a cyber attack, a comprehensive literature review was completed. The purpose of a literature review is to find, read, and analyze the body of literature about a particular topic in order to demonstrate familiarity and establish creditability with the research in the respective field under study (Blum & Muirhead, 2005). The literature review should build on the work of other researchers while establishing the trends and gaps in the existing body of research (Neuman, 2005). For this research study, a review of the historical and current literature on cyberspace, cyber and traditional warfare operations, decision theories, complexity and uncertainty theories, deterrence theories, as well as the legal aspects of cyber warfare was accomplished. The scope of the literature review was focused on the problem statement and purpose of the research study using key terms provided in Appendix A.

Peer reviewed research articles were obtained primarily from University of Phoenix's electronic databases, including EBSCO, ProQuest, Sage, Emerald, and Gale PowerSearch. DoD articles, reports, and studies were accessed from the Defense Technical Information Center (DTIC) databases. Articles and excerpts from books,

magazines, and newspapers were obtained from local public and university libraries. Google™ was the primary Internet-based search engine used for retrieving documents from industry, government, and academic websites. Literature searches were conducted and applicable research was found in 513 titles including 208 peer reviewed journal articles, 80 government and technical reports, 100 books, 42 articles from edited volumes, 26 papers from symposium or conference proceedings, 12 dissertations, 7 monographs, 22 articles from magazines and newspapers, and 16 Internet website articles. Of the 319 peer reviewed titles used for the literature review, 196 (61%) were published within the last five years. The literature limitations and research gaps relating to the uncertainty that military officers encounter when making response decisions following a cyber attack are presented in the conclusions section of chapter 2.

Review of the Literature Strategy

Figure 1 illustrates the research strategy used for conducting the review of the literature. The review of the literature was completed using four overarching themes: background material, cyber warfare, theoretical framework, and legal aspects. The order in which these themes appear in the literature review was selected specifically to enhance the understanding of a complex topic in a highly specialized profession. The first portion of chapter 2 is devoted extensively to setting the stage for the literature review by establishing a standard lexicon and a common frame of reference.

The level and detail of the background material was necessary for three reasons. First, many users including individuals, companies, institutions, militaries, and governments share and conduct activities in cyberspace. Therefore, the background material established clear lines of demarcation that ensured the literature review context

was properly bounded to cyber warfare activities and the associated decision-making processes. Second, given the nascent nature of the research topic, sufficient background material was devoted to describing and differentiating cyber warfare from other traditional military activities. Last, the body of research regarding decision-making uncertainty is vast. Therefore, extensive background research was necessary to constrain the review of the literature and to develop an appropriate theoretical framework for this research study.

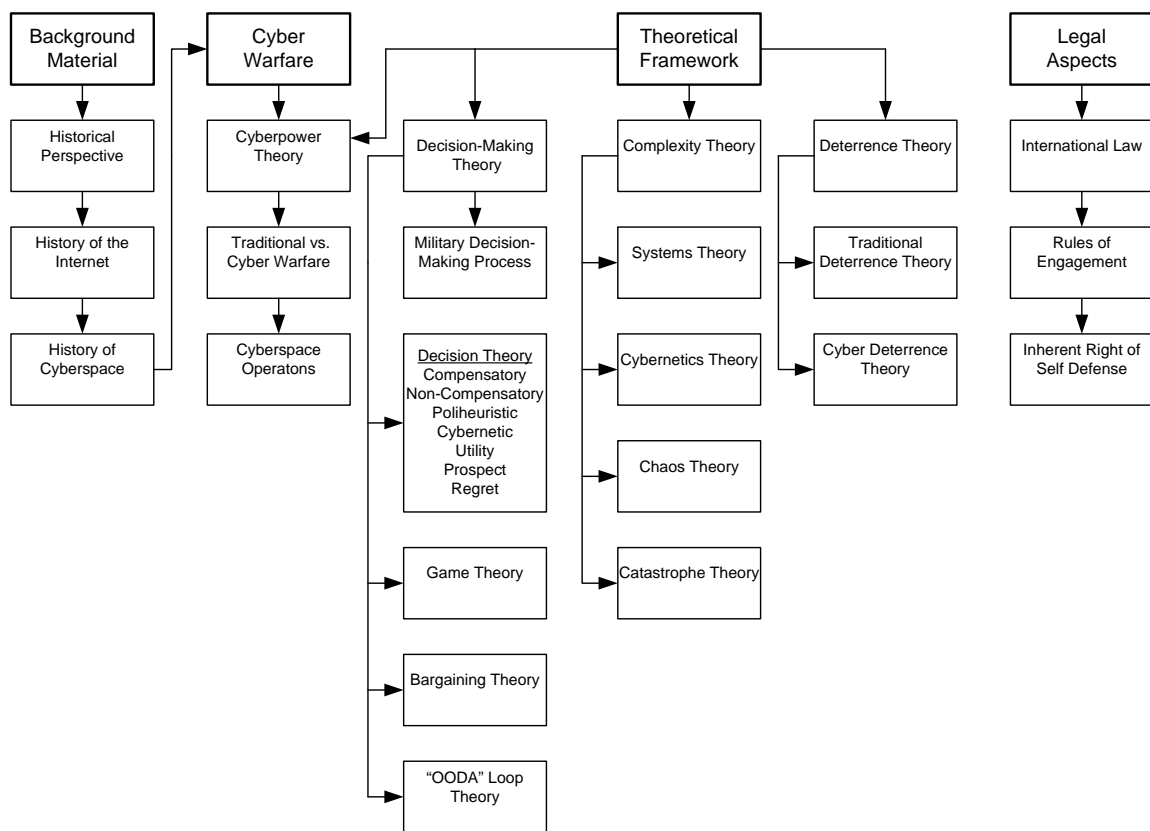


Figure 1. Research strategy for conducting the review of the literature.

Using an historical perspective of the Internet and cyberspace, the digital battlefield is described as the virtual arena where cyber warfare is conducted. Within this context, cyberpower theory is introduced as the governing theoretical construct designed

to conceptualize the strategic decision-making processes associated with cyber warfare activities. To enhance the understanding and application of cyberpower, the principles of war were used to compare and contrast traditional (or conventional) warfare to cyber warfare. Leveraging this comparison, cyberspace operations are defined as a means of expounding on the scope and range of activities currently used to conduct cyber warfare.

Theoretical Framework

The theoretical framework for this research study was developed based on Drucker's (2007) five elements of effective decision-making shown in Figure 2. Decision theory was used to form the fundamental rules and principles required to rationalize the research problem into a generic statement using appropriate and applicable specifications (Drucker, 2007). The problem statement was specified further by using complexity theory to establish the governing boundary conditions. Due to the ubiquitous nature of cyberspace, which is characterized by countless interactive transactions occurring near the speed of light, problems in cyberspace are inherently "wicked" (Churchman, 1967; Rittel & Weber, 1973).

Each wicked problem is "essentially unique . . . has no definitive formulation . . . no exhaustively describable set of potential solutions . . . [and] no ultimate test for a given solution" (Rittel & Weber, 1973, pp. 161-164). Therefore, complexity theory is used to describe the nature of a wicked problem and delimits the set of potential actions that meet the associated boundary conditions. Complexity theory has been shown to be the preferred theoretical construct for approaching wicked problems typically encountered in irregular warfare (Smith, 2009). This is particularly useful because cyber warfare is "the epitome of irregular warfare" (Kehler, 2009, p. 8).

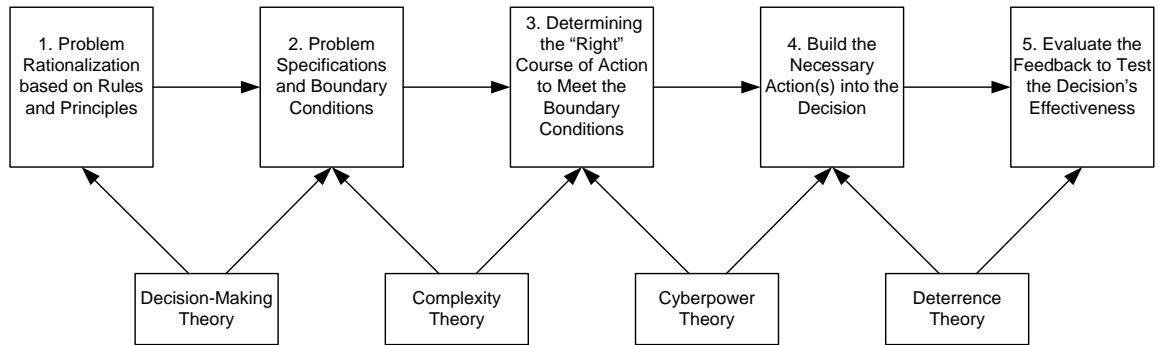


Figure 2. Theoretical framework based on Drucker's (2007) five elements of effective decision-making.

Kramer et al. (2007) proposed cyberpower theory to describe how cyber capabilities could be leveraged as an instrument of national power. Therefore, when determining the appropriate response to a cyber attack, Kramer et al. suggested decision-makers use cyberpower theory to develop the "right" set of actions to be evaluated. Furthermore, by understanding cyberpower theory, leaders can build action into the decision process by considering national and military policy across tactical, operational, and strategic lines of influence and empowerment (Kramer et al., 2007).

To achieve the desired end state, the set of potential actions the decision-maker should consider to dissuade or prevent a cyber attack is refined using deterrence theory (Chesser, 2007; Keyes et al., 1997; Kugler, 2009). The United States reserves the right, according to President Bush (2003), to respond as appropriate considering all elements of national power. Given this national policy, the United States requires an enduring cyber deterrence strategy that is contingent upon the ability to make informed and proportional defense response decisions. Bridging the gap between decisional action and the subsequent response, deterrence theory served as the appropriate theoretical construct for evaluating the effectiveness of cyber warfare decisions.

The review of the literature ends with a review of the legal aspects of cyber warfare. Determining the appropriate response to a cyber attack is inherently a legal decision. Sharp (1999a) established the use of force and the laws of armed conflict apply even when attacks occur in cyberspace. Although an attack that occurs between two nation states is a function primarily of its scope, duration, or intensity and not the medium in which the attack occurs, Sharp expressed marked differences exist between the uncertainties associated with the decision-making processes for authorizing a response action following a cyber attack compared to a traditional kinetic attack.

The legal differences between criminal activities, cyber terrorism, and nation-state sanctioned cyber warfare are explored and distinguished during the literature review. At the national level, making a decision to respond with force requires a comprehensive legal understanding of international law and treaties. Because cyber warfare decision-making was approached in this research study from a military perspective, the literature review also includes an evaluation of the rules of engagement and the inherent right of self-defense.

Historical Perspective

Technology has always been an integral component of warfare (Bull, 1991). From the time when the first warrior used a stone to increase lethality in hand-to-hand combat to the unimaginable destruction caused by thermonuclear devices, technologies have affected the balance of power (Tubbs et al., 2002). In consideration of all technologies, according to Tubbs et al. (2002), communication methods and information-related technological advances have arguably had the most impact in shaping warfare. Throughout the ages, the ability to collect, control, and disseminate information through

the mastery of information technologies has been critical in achieving tactical and strategic advantage in combat. Since the use of communication drums and horns as early as 3000 BC to the high-speed wireless networks in use today, cyberspace technologies (e.g., computers, telecommunications, satellites, and fiber optics) enable command and control of military forces by providing decision-makers rapid, accurate, and secure information (Davis, 2000; Huurdeman, 2003; Tubbs et al., 2002).

History of the Internet: Building the Digital Battlefield

The Internet is a distributed system of computer and telecommunication networks that enables communication, collaboration, and coordination on a global scale (Abbate, 1994). Expanding and evolving more rapidly than ever imagined, the Internet has become the digital infrastructure that supports electronic commerce, broadcast media, financial markets, academic research, as well as military and intelligence operations (Murphy, 2001; Pace, 2006a; Papp & Alberts, 1997). In this section, the concept of viewing the Internet as a digital battlefield is introduced by presenting the history of (a) computer networks, (b) the ARPANET, (c) the Internet, and (d) the World Wide Web (WWW).

Computer networks. Leiner et al. (1997) said, “The Internet has revolutionized the computer and communications world like nothing before” (p. 102). Understanding the contributory importance of the telegraph, telephone, radio, and computer with respect to the Internet’s unparalleled assimilation of information technologies, the father of the Internet, Cerf (1989), in the *Requiem for the ARPANET*, wrote:

Like distant islands sundered by the sea,
we had no sense of one community.

We lived and worked apart and rarely knew
 that others searched with us for knowledge, too
 But, could these new resources not be shared?
 Let links be built; machines and men be paired!
 Let distance be no barrier! They set
 that goal: design and build the ARPANET! (p. 27)

According to Abbate (1994), a universal interest in computer accessibility forced global network construction, which created Cerf's interconnected "distant islands," generating a social networked system of shared knowledge.

As envisioned by Cerf (1989) and highlighted by Abbate (1994), the need to network is a social phenomenon. Pinch and Bijker (1987) proposed that new technologies often exhibit "interpretive flexibility" with amorphous structures based on indeterminate social and cultural utility. As relevant social groups with shared technological meaning form a "critical mass" and adopt a particular design consistent with their goals, a stable network construction emerges (Abbate, 1994). Understanding how social factors influenced the development of networks is useful in explaining the design variations observed as the Internet evolved. Therefore, the design of computer networks resulted from decisions that reflected the resource constrained goals of relevant social groups, which included computer owners, information technology manufacturers, and telecommunication providers (Abbate, 1994; Laursen, 2007; Leiner et al., 1997).

In 1963, Licklider conveyed the "Galactic Network" concept by proposing the level of social interactions that was achievable through international computer network integration designed to ensure prompt, convenient, and easy accessibility to computer

programs and information. While Licklider was envisioning how computers would one day connect people through a social medium, Kleinrock (1962) completed the germinal work on packet switching theory (Leiner et al., 1997). Packet switching is a process that decomposes a message down into separate, discrete packets prior to transmission (Federal Communications Commission [FCC], 2007). Each packet travels from its originating point to its termination point over any available route, independent of the path taken by the other packets. After the packets arrive at their destination, another process reassembles them to form the original message (FCC, 2007). With Licklider's social connectivity concept and Kleinrock's theoretical packet switching theory in place, the last step was to develop the technologies necessary to support communication between multiple computer devices including a variety of computers built by numerous companies with distinctive operating systems (FCC, 2007).

In 1965, Marill and Roberts connected a TX-2 computer at Lincoln Labs in Cambridge, Massachusetts with a Q-32 computer at System Development Corporation in Santa Monica, California (Abbate, 1994). To establish the connection, Marill and Roberts used a low-speed dial-up modem and their own software across a leased line from Western Union (Abbate, 1994; Leiner et al., 1997). Through this experiment, Marill and Roberts (1966) proved two computers could time-share successfully by running simultaneous programs, sharing data files, and accessing remote machines; however, the circuit-switched telephone system's capacity was completely inadequate without Kleinrock's packet switching process (Leiner et al., 1997).

ARPANET. In 1967, the DoD contracted with the Advanced Research Projects Agency (ARPA) for the "purposes of studying the design and specification of a computer

network” (FCC, 2007, p. 35). From the \$19,800 contract, the ARPANET emerged as the precursor to the Internet (FCC, 2007). Chartered to regain U.S. technical superiority in response to the Soviet Union’s advances in warfighting hardware and space exploration, ARPA realized the synergy of harnessing the brainpower dispersed throughout the academic institutions would require substantial advances in computer networking (FCC, 2007). By 1968, the DoD committed \$563,000 for the purpose of developing, installing, and experimenting with four interface message processors (IMPS) called ARPANET switches (FCC, 2007; Leiner et al., 1997). The ARPANET team used the IMPS to link computers at the Stanford Research Institute, the University of California-Los Angeles (UCLA), and the University of Utah (FCC, 2007). Finally, on October 15, 1969, on the second attempt, the IMPS installed at UCLA and Stanford University made a revolutionary connection with the words “log in” (FCC, 2007, p. 36).

Internet. The ARPANET soon transformed into the Internet due to the vision of a “galactic” social network empowered by packet switching theory, a suite of standardized protocols, and a rapidly evolving information technology infrastructure fueled primarily by the telecommunication market (FCC, 2007). Leiner et al. (1997) defined the Internet as a “worldwide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location” (p. 102). By 1972, ARPA, later renamed DARPA (Defense Advanced Research Projects Agency), established four requirements for the Internet’s open-architecture design:

1. Each distinct network had to stand on its own, and no internal changes could be required of any such network before connecting to the Internet;

2. Communications would be on a best-effort basis. If a packet failed to arrive at the final destination, the source would retransmit the packet as quickly as possible;
3. 'Black boxes' (later called gateways and routers) would be used to connect the networks. The black boxes would not retain information about individual flows of packets passing through them. Therefore, the black box design would be simple while avoiding complicated adaptation and recovery from various failure modes; and
4. There would be no global control at the operations level. (Leiner et al., 1997, pp. 102-103)

These design requirements formed the basis for the Internet governance model, which remains valid and applicable today.

The ARPANET model had a three-layer design. Specifically, the model had an *application layer* to handle user activities, file transfer, e-mail; a *host layer* to set up communication between host processes; and a *communication layer* to move data through subnet using packet switching (Abbate, 1994). The host-layer protocol, originally referred to as the Network Control Program (NCP), allowed connections to be established independent of any particular host service application (e.g., remote login, file transfer; Abbate, 1994). Leveraging their experience with the NCP, Cerf and Kahn developed the Transmission Control Protocol/Internet Protocol ([TCP/IP]; Leiner et al., 1997). After TCP alone failed to handle network traffic efficiently, IP was necessary to improve performance to an acceptable level.

To improve this limitation, Cerf and Kahn designed TCP to handle flow control and lost packet recovery while IP provided addressing and forwarding of individual packet services (Leiner et al., 1997). Because the Internet was designed as a common infrastructure based on its ARPANET origins, TCP/IP's general service nature facilitated the emergence of new applications such as the WWW. By 1980, the DoD declared TCP/IP as the Internet standard for sharing DARPA Internet technology to the DIB (Dellums & Bingaman, 1993; Leiner et al., 1997). As the number of nodes and networks continued to grow, the Internet, by 1985, supported a broad community of researchers, developers, and businesses as the primary method of daily computer communications. E-mail services and bulletin board forums emerged as the social networking applications of choice. The popularity of networked connectivity soared as the Internet subsumed more than 50,000 networks globally with 29,000 networks in the United States alone (Leiner et al., 1997).

World Wide Web. Burners-Lee invented the WWW (or the “Web”) in 1989 while working as a research scientist at the Geneva-based European Center for Particle Physics, known by its French acronym, CERN (Conseil Européen pour la Recherche Nucléaire; Aikat, 1995). Burners-Lee conceived and developed the Web to “meet the demand for automatic information sharing between scientists working in different universities and institutes all over the world” (CERN, 2008, para. 1). Berners-Lee and Cailliau refined the original Web concept when they submitted a proposal the next year entitled *World Wide Web: Proposal for a Hypertext Project* (Laursen, 2007). The WWW was installed at CERN in 1991 when Berners-Lee and Cailliau (1990) specified the Hypertext Markup Language ([HTML]; Aikat, 1995).

Berners-Lee and Cailliau (1990) are responsible for developing three standards that define the Web as a unique Internet communication medium:

1. Uniform Resource Locators (URLs) - Each Web page has a unique Internet address known as a URL;
2. Hypertext Markup Language (HTML) is the standard language for highlighting documents with URLs to connect them to other documents on the Web; and
3. Hypertext Transfer Protocol (HTTP) is the standard for transferring hyperlinked documents from Web servers to clients via the Internet. (Aikat, 1995, pp. 8-9)

Although established in 1989 and implemented in 1991 as an Internet-based medium for scientists to share information globally, the Web did not begin to become popular until 1993 when software companies developed browsers designed to simplify the commands required by the HTML and HTTP standards (Aikat, 1995).

In 1992, Johnson, a physicist at Stanford Linear Accelerator Center (SLAC) released the “MidasWWW” browser, which was capable of viewing PostScript files via the Internet from both UNIX and Virtual Memory System (VMS) machines (Deken, 2006). By 1993, according to Gillies and Cailliau (2000), the release of the Mosaic computer program browser by the National Center for Supercomputing Applications (NCSA) initiated profound changes in the use of the Internet from an educational environment to a wide-scoping communication platform. Designed by Andreessen and Bina, Mosaic was the result of funding sources associated with the *High Performance Computing and Communications Act* of 1991 (i.e., *The Gore Bill* named after then Senator Al Gore; Deken, 2006; Perine 2000). Mosaic embodied the Internet’s design

features, including TCP/IP-based URL communications, native HTTP, Gopher (search and retrieval network protocol), file transfer protocol (FTP), and network news transfer protocol (NNTP), all packaged in an advanced graphical user interface (GUI) for the Microsoft Windows, Apple Macintosh, and Unix X-Window operating systems (Andreessen & Bina, 1994).

The popularity of Mosaic was unprecedented. Mosaic, as described by Andreessen and Bina (1994), presented the user with a “single, unified interface to all this functionality [with] complete transparency of the data location and retrieval process” (p. 11). Designed to avoid encumbering the user with the technical details of information navigation and retrieval, Mosaic permitted the user to concentrate on the real task of interacting with the information itself. According to Hudson (1997), Andreessen’s conceptualization of Mosaic coupled with the work of hypertext theorist Berners-Lee (1989) is generally acknowledged as the beginning of the Web as currently recognized. Unfortunately, by 1994, Mosaic began to lose popularity following the release of more capable browsers such as Netscape Navigator and Microsoft Internet Explorer, both of which were derived from Mosaic source code (Hardmeier, 2005; Hudson, 1997).

History of Cyberspace

Cyberspace has numerous definitions, interpretations, and applications depending on the stakeholder (Kuehl, 2009). However, similar among these characterizations, cyberspace is complex, interdependent, networked, technological, operational, and virtual (Bush, 2003; Kuehl, 2009; Murphy, 2001). In this section, cyberspace is described as a domain of warfare. This description was developed by stepping through the evolution of

the current construct using the following sections: (a) origins, (b) national recognition, and (c) declaration as a warfighting domain.

Origins. Thus far, a systematic approach has been used to present the necessary building blocks of cyberspace. Specifically, telecommunication systems, computer hardware and software, a Web empowered Internet, electromagnetic energy, and most important, the users provide the necessary and sufficient technological and societal components that form cyberspace. Therefore, cyberspace and the Internet are not equivalent constructs. Gibson (1984) introduced the concept of cyberspace in the science fiction novel *Neuromancer*:

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace [sic] of the mind, clusters and constellations of data. Like city lights, receding (p. 69)

In this famous passage, Gibson captured the technical, social, cultural, and cognitive nature of cyberspace as a virtual construct of distributed networks. According to Murphy (2001), Gibson envisioned a time when there would be no clear boundary between the human mind and digital knowledge networks.

Cyberspace recognized nationally. By 2003, the U.S. dependence on cyberspace was undisputable. In recognition of the nation's critical infrastructure dependency on cyberspace, President Bush (2003) published *The National Strategy to Secure Cyberspace*. Within this strategy, Bush defined cyberspace as the control system of the

country. Specifically, cyberspace is “composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security” (Bush, 2003, p. vii). Written as an enabling component of the U.S. government’s responsibility to provide for homeland defense with emphasis on the protecting critical infrastructures and essential services, Bush stressed the importance of empowering Americans to take personal action to safeguard the cyberspace resources they utilized. This perspective provides valuable insight into the nature of cyberspace and the differences between cyberspace and the original Internet construct.

Cyberspace as a new warfighting domain. Responsible for defending the GIG (i.e., military command and control systems) and the DIB, the CJCS, General Pace published the *National Military Strategy for Cyberspace Operations* in 2006. Pace (2006a) established a military strategic framework designed to orient, focus, and integrate cyber warfare activities across the DoD including intelligence gathering and business operations. Within this strategy, Pace defined cyberspace as “a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures” (p. ix). For the first time, the DoD recognized cyberspace as a warfighting domain, equal to land, sea, air, and space from the perspective of developing military forces, programming and budgeting resources, as well as operational planning and execution.

From 2003 until the end of 2007, the U.S. government had done little to develop initiatives capable of securing cyberspace as envisioned by the president’s 2003 strategy.

Finally, in January 2008, the president signed the National Security Policy Directive (NSPD) 54/Homeland Security Policy Directive (HSPD) 23, a comprehensive national cyberspace program designed to improve the security, resiliency, and reliability of U.S. networked systems and critical infrastructures against cyber attacks (Chertoff, 2008). The president's policy directive to secure cyberspace is a collaborative interagency initiative planned and implemented by all federal government departments and agencies.

Deputy Secretary of Defense England (2008a) established a new definition of cyberspace to align and synchronize the DoD's cybersecurity efforts. Specifically, England defined cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (p. 1). The new definition more precisely quantifies the fundamental building blocks of cyberspace, which allows the DoD to mature cyberspace as a warfighting domain by properly training, equipping, and organizing cyber forces in addition to developing cyber capabilities (England, 2008a).

Cyber Warfare

An integral and important element of understanding military decision-making process (MDMP) and theory in cyberspace is the concept of cyber warfare (Alford, 2000; Saunders & Levis, 2007). Cyber warfare is the conduct of traditional warfare operations in and through cyberspace (Alford, 2000; Carr, 2010; Clarke & Knake, 2010; Heickerö, 2006). In this section, cyber warfare is described by (a) background material, (b) cyberpower theory, (c) social and cultural aspects, (d) behavioral and cognitive aspects, (e) ethical aspects, and (f) technical aspects.

Background. Prior to Post's (1979) term "cyber war," Rona (1976) defined the term "information warfare" in the early 1970s while studying control system dynamics and interactions, a field known as *cybernetics*. Rona described the competitive relationship between linked control systems as a type of information warfare. Rona contended that control systems compete to gather, process, and disseminate information via flow and feedback paths of extraordinary complexity. In 1993, the DoD published an official and classified definition of information warfare that evolved and changed over time as operational capabilities improved. By 1997, the DoD had defined information warfare as "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (Kuehl, 2002, p. 36). However, in October 1998, the CJCS, General Shelton (1998) published Joint Publication 3-13, *Joint Doctrine for Information Operations*, which eliminated the definition of information warfare by including its conceptual meaning in the definition of information operations (IO). Specifically, Shelton defined IO as the "actions taken to affect adversary information and information systems, while defending one's own information and information systems" (p. I-9).

Due to the complexity of predicting second and third order effects when conducting IO, Shelton (1998) emphasized the need to integrate offensive and defensive capabilities while carefully monitoring the associated activities using robust command and control processes enabled by intelligence support. Therefore, from an IO frame of reference, the introduction of electronic attack (EA) and CNA established the first natural linkage between information and cyber warfare. Although conducted with similar assets, capabilities, and skills, the DoD plans and executes IO and cyberspace operations as

different warfighting disciplines with separate rules of engagement and budgeting processes.

In *The National Military Strategy*, the CJCS, General Myers (2004) asserted, “The Armed Forces must have the ability to operate across the air, land, sea, space, and cyberspace domains of the battlespace” (p. 18). Due to the reliance on cyberspace to achieve national objectives in the areas of military, intelligence, and business operations, the DoD must be able and ready to conduct cyber warfare as a means of exploiting cyberspace to gain strategic, operational, and tactical advantage over adversaries (Pace, 2006a). In this context, Hildreth (2001) defined cyber warfare as “warfare waged in cyberspace” (p. CRS-16). Cyber warfare includes protecting data, computer systems, and associated infrastructures against malicious intrusions in order to ensure “freedom of action” in the contested cyber domain while denying the same to adversaries (Hildreth, 2001; Pace, 2006a). According to Sharp (1999a), a cyber attack is a CNA or some other state sponsored activity in cyberspace that causes an effect that invokes that state’s inherent right of self-defense.

Janczewski and Colarik (2008) defined cyber warfare (also referred to in the literature as information warfare) as a “planned attack by nations or their agents against information and computer systems, computer programs, and data that results in enemy losses” (p. xiv). Due to the nature of cyberspace, which is empowered by its global prevalence and low cost of connectivity, countless actors can easily participate in malicious activities that scale in severity within this virtual domain. Among these activities, cyber crime, cyber terrorism, and cyber warfare are the most concerning for decision-makers in terms of potential harm, sophistication, legal authority, and

appropriate response actions. While each of these activities is addressed in this study where appropriate, cyber warfare is the focus of this section. With this in mind, cyber warfare is a traditional military activity that uses computer network tools, tactics, and techniques as combat weapons designed to attack authorized groups of people, property, and economic resources (Owen, 2008).

The question remains if cyber warfare is a legitimate warfighting discipline. To a large degree, this question is answered best from a legal perspective, which is presented in later sections with substantial detail. However, a logical Clausewitzian argument can illuminate this issue. Clausewitz (1873) characterized war as “an act of [physical] force . . . a pulsation of violence . . . to impose our will” (p. 47). Therefore, the purpose of force and violence is to impose the will of one political entity onto another political entity (Kuehl, 2002). In the Clausewitzian paradigm, a class of actors called “warriors” wage war in loyal support of political entities called “States” (Kuehl, 2002, p. 47).

With regard to Clausewitz, Kuehl (2002) suggested nation states recognize they are at war when an attack reduces their military capacity, damages their essential infrastructures, and introduces chaos into their political and economic systems. Therefore, cyber warfare is a legitimate warfighting activity if cyberspace operations are considered a legal use of force sanctioned by a sovereign State. If Clausewitz’s (1873) assertion that “war is nothing but the continuation of policy with other means” (p. 69) is valid, then a nation state’s employment of *cyberpower* during war is a lawful way to achieve legitimate political ends.

Cyberpower theory. Jordan (1999) developed a theory of cyberpower based on three interconnected regimes: power from an individual’s viewpoint, a social perspective,

and the collective imagination. According to Jordan, understanding cyberpower requires a thorough grasp of the theories of power. Therefore, Jordan built a cyberpower theory based on “Max Weber’s common sense theory of power as the possession of individuals, Barry Barnes’ theory of power as the constituent of social order, and Michel Foucault’s analysis of power as domination” (p. 4). On an individual level, cyberpower is the product of “identity fluidity, the remaking of hierarchy, and spaces made out of information” (Jordan, 1999, p. 5). These three dimensions form a cyberpower framework comprised of “access, privacy, encryption, copyright, and censorship that offers power [in cyberspace] to the individual” (Jordan, 1999, p. 5).

Over time, users interacting in cyberspace begin to experience a level of commitment to their respective communities that surpasses their individual belief systems. In turn, these communities begin to set conditions and behavioral patterns for the virtual existence of individuals in cyberspace (Barzilai-Nahon & Neumann, 2005). Jordan (1999) asserted that cyber societies are built on the virtual presence of users enabled by information and communication technologies constructed and networked according to social values. Social power stems from the capability to master the networks of information technology as inert objects, and this ability, according to Jordan, is determined by expertise.

The final fundamental perception of Jordan’s (1999) cyberpower theory flows from the realization that the types of interactions and tools experienced in cyberspace are as important as the commitment to a particular cyber society. Jordan theorized that the union of individuals and societies in cyberspace is the result of a “collective imagination” through which users, at first unfamiliar with each other, become committed to a common

virtual community. The collective imagination of cyberspace is manifested on the premise of two disparate realizations along the cognitive spectrum. On one end, some believe the virtual world of cyberspace brings the opportunity for “immortality and the final ascension of humanity into godhood” (Jordan, 1999, p. 7). On the other end, some fear cyberspace provides the ultimate window into their private lives enabled by the perfect surveillance tool capable of creating the ideal totalitarian society (Jordan, 1999). According to Jordan, cyberpower becomes formidable when the individual, social, and cognitive forces coalesce through the interrelation of the three fundamental levels of the virtual social order.

With the 2006 Quadrennial Defense Review, Secretary of Defense Rumsfeld acknowledged a “compelling need for a comprehensive, robust, and articulate cyberpower theory that describes, explains, and predicts how our nation should best use cyberpower in support of U.S. national and security interests” (Kramer et al., 2007, p. 1). In the year that followed, researchers for the National Defense University’s Center for Technology and National Security Policy completed a study designed to create a strategic framework for describing cyberpower. In this study, Kramer et al. (2007) defined cyberpower as the “ability to use cyberspace to create advantages and influence events in the other operational environments and across the elements of national power” (p. 4).

Current cyberpower theory is based on a three-layer framework (Kramer et al., 2007). Visualized as a pyramid, cyberspace and the supporting technology-enabled infrastructures form the first or foundational layer. Kramer et al. (2007) characterized this level with MoPs such as connectivity parameters, bandwidth, and number of intrusions prevented. Building on this foundation, the levers of power (e.g., diplomatic,

information, military, and economic) create the second layer. Kramer et al. asserted that MoEs such as those associated with military operations or economic sanctions best describe how changes in cyberspace influence the levers of power. The third and final layer addresses to what extent variations in cyberspace empower key entities. According to Kramer et al., these entities include “individuals, activists, terrorists, transnational criminals, nation states, and supra-national organizations (e.g., The United Nations)” (p. 4). MoEEs (i.e., the extent to which an entity can perform key functions and missions due to the capability afforded by cyberpower) characterize the final layer of the framework (Kramer et al., 2007).

In general, MoEs and MoPs are not the same and provide different insights into a system’s behavior. According to Bullock (2006), a MoE relates to “how well a system tracks against its purpose or normative behavior” (p. 20). However, a MoP, or as often referred to a measure of efficiency, establishes how well a “system utilizes resources” (Bullock, 2006, p. 20). Bullock summed up these ideas by stating a “MoE determines if the right things are being done and a MoP determines if things are being done right” (p. 20). A simple input \Rightarrow output \Rightarrow effect model provides the best visualization of the relationship dynamics. If the inputs yield the required outputs, the MoP is met. If the inputs yield the desired effects, the MoE is met. Therefore, the mapping process from a MoP to a MoE is scenario dependent.

The final component of a comprehensive cyberpower theory is a crosscutting institutional and policy matrix that transcends each layer. Factors such as governance, legislative considerations, government-corporate responsibilities, and partnerships form a connective element that binds the three layers into a comprehensive framework (Kramer

et al., 2007). From a governance perspective, organizations such as the Internet Governance Forum (IGF) and the Internet Corporation for Assigned Names and Numbers (ICANN) help establish international norms with regard to Internet security, unwanted solicitation, restrictions, censorship, jurisdiction, and permission requirements for “fair use” of copyrighted material (Kramer et al., 2007).

Legally, two important considerations emerge fundamental to a nation’s application of cyberpower. These issues are based on *jus ad bellum* (law of conflict management) and *jus in bello* (law of armed conflict), which help decision-makers legally determine what constitutes an armed attack in cyberspace and when a use of force would be appropriate (Sharp, 1999a). Last, establishing how to protect the nation’s critical infrastructures is extremely important when understanding cyberpower. Among the 18 infrastructures defined as “critical,” the electrical power grid, the banking industry, and the telecommunication networks are the most vulnerable due to their inherent dependency on the Internet, susceptibility to cyber attack, and the cascading effects they have on other infrastructures (Kramer et al., 2007; Moteff & Parfomak, 2004).

Social and cultural aspects. Borgmann (2004) believed that cyberspace allows entrance into an elusive virtual reality that marginalizes authenticity and contextual meaning. Although this position is arguably debatable, the Internet has catalyzed a new sociological phenomenon among users of technologically enabled connectivity (Fox, Arena, & Bailenson, 2009). Brachman (2006) observed that innovative social activities are utilizing cyberspace assets with safeguarded measures to encourage business ventures, promote social interactions, and stimulate creative thinking while endorsing independent actions with the goal of developing a communal ideology. Therefore, as

Brey (2006) noted, many social and cultural implications exist that shape how society thinks about and interfaces in cyberspace.

Although societal demands can shape technology, designers can reconfigure technology to influence and, to a certain degree, control sociological and cultural consequences. Brey (2006) termed this control process “technological delegation” (p. 47). Using methods such as value-sensitive design can explicitly steer redesign and reconfiguration efforts (Nissenbaum, 1998). In addition to these strategies, changing the way society uses technology within a given social setting or context can have substantial effects. For example, an organization can regulate Internet usage through policies. Brey described this process “structuration” (p. 47). Last, Brey asserted that “assigning different meanings to a technology, both denotative (regarding its form and function) and connotative (regarding its emotional and figurative meaning),” (p. 47) changes the way society interprets and understands that technology. Brey labeled this observation “signification” (p. 47).

Within the context of cyber warfare, adversaries use social engineering techniques strategically to manipulate the thoughts and opinions of people within a social networking group in order to create uncertainty about the ability to demonstrate adequate security and protection (Aiello, 2008). Essentially, social engineering is the employment of perception management techniques (Aiello, 2008). As a cyber warfare enabler, social engineers manipulate targeted individuals or groups to take actions or reveal private information that facilitates further adverse motives. According to Aiello (2008), this process usually requires developing trust with potential victims by relaxing their psychological state, which later renders them more vulnerable to the adversary’s real

desires. Typically, social engineers conduct their attacks in person, over the phone, or via e-mail.

Sun Tzu (n.d./1910) believed, “All warfare is based on deception” (p. 5). Social engineering exploits this concept. Gaining access to a network is challenging and vital to conducting cyber warfare. As an example, an attacker conducts the first phase of a cyber attack by convincing a user to open a malicious e-mail attachment related to a comfortable and enticing topic (Aiello, 2008). Once opened, the attachment easily defeats the network’s firewall, intrusion detection system, and other defensive tactics. Aiello (2008) warned that military facilities with cyber resources should prepare for socially engineered attacks by ensuring users are aware of such cyber warfare tactics.

Behavioral and cognitive aspects. Related to the social aspects of cyberspace described above, behavioral and cognitive aspects require further elaboration within the context of cyber warfare. Zimet and Skoudis (2009) described cyberspace as comprised of an architectural element (e.g., transport, services, applications), information (e.g., data, content), and a human element (e.g., cognitive, culture, behavior). Pace’s (2006a) description of the information environment is closely related to Zimet and Skoudis’ characterization of cyberspace. In *The National Military Strategy for Cyberspace Operations*, Pace asserted that the information realm is comprised of three essential components, namely physical, cognitive, and informational dimensions. The cognitive dimension is vital for understanding how people decide to use the physical and informational dimensions in cyber warfare.

Appropriate and constructive behavior by users of cyberspace can enhance the safeguarding of information whereas improper and harmful actions can severely

undermine the designed protective mechanisms (Stanton, Stam, Mastrangelo, & Jolton, 2004). According to Fagnot (2008), recognizing the human factors associated with cyberspace must be the first step in building a robust information security posture. While cyber attacks by external adversaries are more publicized, Nguyen, Reiher, and Kuenning (2003) argued that attacks by insiders are often more insidious, widespread, and cause greater destruction. Schultz (2002) compiled definitions from Shumway and Einwechter to define an insider attack as the intentional misuse of computer systems by entrusted users with authorized access for the purpose of exploiting, damaging, or stealing sensitive information. Fagnot agreed with Schultz with the warning that “insiders” with the capability, the motive, and the opportunity to commit an attack greatly enhances cyber warfare efforts from outside organizations.

As a means of predicting the behaviors normally exhibited by insiders with access to computer systems, Stanton et al. (2004) developed a classification system depicting end user conduct and categorizing activities that affect network security. In this two-factor taxonomy, Stanton et al. used expertise (high and low) versus intentions (malicious, neutral, and beneficial) to rank behavior factors in order to describe potential risk to an organization. From intentional destruction to detrimental misuse to naïve mistakes, Stanton et al. believed an organization’s cybersecurity procedures and practices must match their behavioral taxonomy structure. Because human behaviors are complex, Fagnot (2008) concluded a deeper understanding of how these behaviors impact information security within an organization is required.

In addition to behavioral factors, cognitive factors have an extremely important role in the conduct of cyber warfare. Heickerö (2006) suggested understanding combat in

cyberspace, conducting network centric warfare, and employing IO within the cognitive domain are essential concepts for the modern warrior. In comparison to the information arena, Heickerö asserted that the cognitive domain is where consciousness originates. In addition to emotions and perception, cognition forms the foundational creative basis for developing characteristics and capabilities associated with leadership, doctrines, and tactics (Heickerö, 2006). Therefore, cognition, perception, and emotion establish the cognitive domain.

Nunes (1999) argued physical, syntax, and semantic effects occur in cyber warfare. Destructive attacks (e.g., directed energy, electronic warfare, and electromagnetic pulse) on information technology infrastructures cause physical effects. Logical attacks on information systems (e.g., viruses, worms, and Trojans) that delay information flow or induce unpredictable behavior cause syntax effects. Deceptive attacks (e.g., psychological operations) that reduce trust and confidence in the vital information required for decision-making cause semantic effects. Therefore, Heickerö (2006) suggested successful digital attacks are asymmetric, anonymous, have effects in the physical world, and influence cognitive, perceptive, and emotional processes that result in decreased situational awareness for the decision-maker.

Ethical aspects. As with all warfighting areas, the ethical implications of cyber warfare start with laws. International laws of war (*jus in bello*) establish standards to regulate how wars can be legally fought (Rowe, 2007). Because the legal implications of cyber warfare are so important, an entire section is devoted to this topic later in chapter 2. Due to the inherent clandestine nature of cyber warfare, which is conducted primarily in the virtual world of cyberspace, the decision-maker must consider several ethical issues.

First, many people associate cyber attacks with cyber criminal activity such as spam and phishing schemes used for the purpose of fraudulent financial transactions (D. Denning, 2007). Second, for nation states, leaders must decide if penetrating or disabling a computer system of an adversary nation state is ethical and if so, determining the ground rules for conducting such an attack is complex (D. Denning, 2007).

Third, “hacktivism” or the combination of hacking and activism is usually the product of non-state actors with politically or socially motivated agendas (D. Denning, 2007). “Cyberterrorism” results when the attacks are “sufficiently destructive to severely harm or terrorize citizens” (D. Denning, 2007, p. 1). The ethical questions arise when leaders consider conducting a cyber attack against websites that support human trafficking, child pornography, and terrorist support and recruitment. Finally, decision-makers must consider the ethical implications of “hack back” or “active response” actions (D. Denning, 2007). Specifically, determining if a network administrator can stop an ongoing attack by conducting a counter cyber attack is difficult from an ethical position. The ethical dilemma in each of the scenarios presented above requires due diligence in consideration of international and domestic laws while acknowledging the challenges associated with attribution uncertainty and unintended consequences in cyberspace.

Rowe (2007) asserted that national policy makers should begin addressing the ethical problems created by the nature of cyber warfare. Because cyber weapons are uniquely dissimilar and employed much differently compared to traditional weaponry, public perceptions about their use and capabilities can be misguided and misrepresented (Rowe, 2007). Because technology has not advanced to a point in which cyber warriors can target their attacks with exact precision, Rowe warned that collateral damage is a

major concern. For example, the effects associated with a cyber attack against a valid military target could inadvertently spread to a civilian site causing substantial damage to a nation's critical infrastructure (Rowe, 2007). Due to the connectedness of cyberspace, battle damage assessment is difficult. Without this valuable, real time situational awareness, ensuring that authorized cyber attacks are proportional and effective in meeting military objectives is a challenging venture. For these reasons and others that are discussed in the legal section of chapter 2, Rowe suggested leaders must be concerned that "cyber attacks may be prosecutable as war crimes" (p. 105).

Technical aspects. Pace (2006a) purported, "Cyberspace evolves in response to ongoing technical innovation and is the only domain whose underlying structure can be dynamically reconfigured" (p. 4). Pace further advised that the DoD must remain in concert with technological change through sustained and constant training, resourced capability development, and domain expertise. Because cyberspace is complex, leaders and users must have thorough technical knowledge of the continual evolutionary process needed to perform warfare activities within the cyber domain (Pace, 2006a). In addition, when operating and defending the GIG, Pace added that combatant commanders must employ innovative technical and non-technical tactics to minimize the impact of vulnerabilities found in operating systems, software applications, and controlled interfaces.

Schneidewind (2008) asserted that predictive models for understanding the growing number of cyber attacks, which exploit technical vulnerabilities, are needed to counteract the threat posed by cyber warfare. A predictive model can provide the cybersecurity professional with an algorithm for analyzing and evaluating defensive

response options by factoring in potential threats, weaknesses, intrusions, and lag times between events (Schneidewind, 2008). Schneidewind suggested one such risk model incorporates the “relative probability of attack, probability of vulnerability, and consequence of an attack” (p. 231). Models resembling the one suggested by Schneidewind are useful since, according to Jennex (2008), cyber terrorists and criminals are attacking systems using similar techniques available to common hackers. Therefore, understanding the risks posed by the day-to-day intrusions provides valuable insights into the tools, tactics, and techniques used in cyber warfare.

Traditional versus Cyber Warfare Doctrine

Comparing the doctrinal differences between traditional and cyber warfare is useful for understanding warfighting decision-making and associated decision theory (Bartholomees, 2008; Butler, Deckro, & Weir, 2005; Heickerö, 2006). This comparison is conducted most effectively using the joint functions of warfare used to integrate, synchronize, and direct military operations (Builder, Bankes, & Nordin, 1999; Fry, 2008; Pace, 2006b). In this section, traditional and cyber warfare are compared and contrasted using the following concepts: (a) command and control, (b) intelligence, (c) fires, (d) movement and maneuver, (e) protection, and (f) sustainment. With these concepts developed, the section concludes with a description of traditional warfighting decision-making, the need for response thresholds, and effects-based warfare.

Command and control. For traditional military warfare, General Pace (2006b) defined command and control as “the exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of the mission” (p. III-1). Command and control incorporates many tasks in order to improve a commander’s

situational awareness including the flow and preservation of information in addition to evaluating and conveying the readiness of essential weapon control systems (Pace, 2006b). Due to the nature of cyberspace, command and control requires rapid decision-making cycles. Pace (2006a) highlighted that effective command and control in cyberspace integrates, coordinates, and synchronizes cyberspace operations at speeds required for achieving awareness and generating effects. Furthermore, cyberspace operations require robust command and control organizational structures to be successful in a globally connected virtual world without sovereign boundaries.

Intelligence. Intelligence provides commanders with an understanding of the operational environment. According to Pace (2006b), traditional intelligence functions include “planning and direction to include managing counterintelligence activities, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback” (p. xvii). In cyberspace, intelligence gathering is associated with computer network exploitation (CNE). CNE encompasses the facilitation of operational processes, surveillance procedures, and information-gathering techniques against oppositional forces using computer network systems (Crane, 2002; Pace, 2006a). Intelligence, which relies on effective collaboration among the intelligence community (i.e., National Security Agency [NSA], Central Intelligence Agency [CIA], Defense Intelligence Agency [DIA]) and domestic organizations (i.e., Department of Homeland Security [DHS], Federal Bureau of Investigation [FBI]), plays a key role in supporting joint battlespace awareness.

Fires. To employ fires, according to Pace (2006b), is to “use available weapon systems to create a specific lethal or nonlethal effect on a target” (p. III-17). The

functions associated with fires are targeting, fire support, countering air and missile threats, interdiction, strategic attack, EA, and CNA. CNA includes “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves” (Pace, 2006a, p. GL-1).

Traditionally, fires produce material damage; however, commanders can employ other attack means, such as EA and CNA, to achieve desired effects with little to no physical destruction.

Targeting is vital to the concept of fires. Targeting comprises a selection and prioritization process for linking validated targets to the appropriate response action based on strategic objectives, operational requirements, and technical capabilities. Unfortunately, targets in cyberspace can be “fuzzy” due to the uncertainty associated with attribution (Huynh, Nakamori, Ryokey, & Ho, 2007). Consequently, prior to authorizing kinetic or non-kinetic fires, the commander’s planning and legal teams must carefully evaluate the strategic national effects, political implications, and legal authorities when making targeting recommendations (Pace, 2006b).

Movement and maneuver. In traditional warfare, “Movement involves the deployment of forces into an operational area and maneuver is their employment in combination with fires to achieve positional advantage” (Pace, 2006b, p. xviii). Movement and maneuver include “disposing joint forces to conduct campaigns, major operations, and other contingencies by securing positional advantages before combat operations commence and by exploiting tactical success to achieve operational and strategic objectives” (Pace, 2006b, p. III-22). In cyberspace, movement and maneuver have non-traditional characteristics that result from near speed of light global mobility.

The expansive geopolitical boundaries associated with cyberspace's information technology infrastructures and the nearly limitless bandwidth contained in the electromagnetic energy spectrum, information movement can occur instantaneously virtually anywhere (Pace, 2006a). Because cyberspace is a volatile domain with respect to network size, user identity, and technical capability, adversaries have unprecedented maneuverability in this domain. Therefore, cyber warfare targeting processes must be robust, flexible, and adaptive to this dynamic environment.

Protection. In traditional warfare, formidable defensive measures must balance strong offensive capabilities as a means of providing protection for valuable assets, organizations, and relationships. According to Pace (2006b), the protection function safeguards and conserves the joint force's combat power by employing active defensive measures (e.g., air, space, missile defense), passive measures (e.g., concealment, counter-deception, counterpropaganda), in addition to emergency management and response. By effectively integrating protective functions, joint forces and their associated systems and facilities are more difficult to locate and attack; moreover, the unnecessary loss of personnel due to fratricide and accidents is reduced. Ensuring protective measures are in place lowers the risks associated with the "wide range of threats such as terrorism, criminal enterprises, environmental threats/hazards, and computer hackers" (Pace, 2006b, p. III-25).

In cyberspace, protection measures require a spectrum of layered defense measures for maximum effectiveness. CND actions "protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks" (Pace, 2006a, p. GL-1). To accomplish these actions, CND

personnel, according to Pace (2006a), employ information assurance capabilities in response to unauthorized activity based on alert or threat information. Pace defined information assurance as those measures designed to “protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation” (p. GL-2). Because cyberspace assets are vital for the command and control of interoperable military forces, the ability to operate networked systems in a degraded state during a large-scale cyber attack is an essential design element.

Sustainment. Key to all military efforts is the ability to sustain operations. In joint doctrine, sustainment, as defined by Pace (2006b), is the “provision of logistics and personnel services necessary to maintain and prolong operations until mission accomplishment” (p. xviii). Well-established sustainment plans provide the warfighter with endurance to extend operational reach with depth and regeneration time (Pace, 2006b). Sustainment is equally vital to conducting cyberspace operations effectively. Specifically, sustainment measures allow cyber warriors to continue fighting while networked information systems are degraded.

Within this context, sustainment in cyberspace includes “domain resilience, redundancy, and restorative capacity” (Pace, 2006a, p. 10). Through consequence management and continuity of operations (COOP) procedures, decision-makers have more confidence in the credibility and reliability of the information processed through cyberspace (Pace, 2006a). COOP provides the military leaders with the capabilities to continue mission-essential functions without unacceptable interruption to maintain military effectiveness, readiness, and survivability. By sustaining operations through

COOP procedures, Pace (2006a) asserted cyber warriors make better decisions regarding the continued use of an exploited system in order to support on-going or planned military operations.

Traditional warfighting decision-making. “War is a violent clash of interests between or among organized groups characterized by the use of military force” (Krulak, 1997, p. 3). Krulak (1997) further suggested, “The essence of war is a violent struggle between two hostile, independent, and irreconcilable wills, each trying to impose itself on the other . . . [using a] fundamentally interactive social process” (p. 3). Traditional warfare is based on the nine principles of war: objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity (Pace, 2006b). These principles form the traditional military decision-making paradigm. This paradigm, historically based in Sun Tzu and Clausewitzian ideologies, shapes today’s military decision, planning, and execution doctrinal processes including tactics, techniques, and procedures.

Decision-making is both art and science. Pace (2006b) wrote, “Effective decision-making combines judgment and intuition acquired from experience, training, study, and creative thinking. Commanders visualize the situation and make sound and timely decisions” (p. III-2). Therefore, vital to the process of making sound decisions is experience and the ability to visualize the situation. Because cyber warfare is an emerging, non-kinetic, asymmetric warfighting discipline that occurs in a virtual domain, leaders lack experience; moreover, physical effects from the actions they take are not always observable.

According to Sun Tzu (n.d./1910), “Speed is the essence of war. Take advantage of the enemy’s unpreparedness; travel by unexpected routes and strike him where he has taken no precautions” (Krulak, 1997, p. 69). These premises apply in traditional and cyber warfare. Time is a crucial factor when making decisions. In general, the leader who can make and implement decisions more quickly and efficiently gains a substantial advantage (Krulak, 1997). To realize these potential decisional gains, Pace (2006b) asserted that leaders require information management skills, awareness of the operational environment, and decentralized decision-making authority. To be successful in warfare, Krulak (1997) and Pace agreed that leaders must make and execute decisions more rapidly than their adversaries do.

In cyberspace, operating within the decision cycle of an adversary is extremely challenging due to global connectivity empowered by information flow occurring close to the speed of light. Therefore, warfighters must take advantage of cyberspace to accelerate their own decision-making cycle while degrading that of the adversary. To accomplish this, Pace (2006a) strongly recommended the DoD must not only defend cyberspace through robust active defense mechanisms, but must also exploit adversary cyberspace vulnerabilities while gaining a deeper understanding of the enemy’s decision cycle and defensive weaknesses.

Defensive response action thresholds (“Red lines”). Traditional warfare is predicated on the clear and unambiguous ability to make use of force decisions in response to attacks that cross well-defined response action thresholds frequently called “red lines” (Colby, 2007). Brandt (2006) defined red lines “as the proverbial line in the sand” (p. 14) within the context of defensive response decision-making. Red lines are the

“points of no return where an adversary’s acceptable extremes of behavior are defined” (Brandt, 2006, p. 14). Although the decision-maker need not limit the response to military action if a red line is crossed, Brandt asserted that red lines are necessary for establishing credible international lines of demarcation designed to facilitate the willingness to use force if necessary. Traditionally, the president considers all elements of national power when responding to an adversary crossing a red line. These elements include diplomatic, informational, military, economic, law enforcement and intelligence response options (Josten, 2006).

Red lines, the fundamental component of a declaratory policy, can be effective at deterring adversarial actions across a broad range of hostilities (Brandt, 2006).

Unfortunately, an adversary’s decision calculus is extremely complex, which infers that proper behavior will not always result. For this reason, leaders must carefully weigh these considerations when setting red line threshold criteria. Colby (2007) believed a credible deterrence policy must incorporate these criteria effectively. For red lines to be employed successfully, Colby found they must establish clear guidelines that can be governed by legitimate authority, motivated by the proper intent, and fully supported by the U.S. government. Consequently, decision-makers must have the will to execute the declared action with a credible capability if an adversary crosses the red line. According to Brandt (2006), credibility is crucial in making the red line declaration effective.

According to Rattray (2001), the United States should proclaim a “declaratory deterrence policy related to strategic information warfare” (p. 475). Rattray suggested that such a policy would compel government leaders to determine the level of provocative behavior that would provoke a response action. In other words, red lines

against cyber attacks are necessary. However, in cyberspace, establishing red lines is particularly complex for several important reasons including a lack of clear attribution, insufficient technological advantage, and an undefined defensive response action threshold. Even with these challenges, Rattray believed that cyber attacks that result in personal harm or substantial economic impact constitute acts of war. Consequently, the United States should openly declare these acts as hostile and aggressively employ appropriate defense response actions including the use of force. To make this declaration credible, Rattray warned that improved capabilities to discern responsibility for cyber attacks are necessary.

Effects-Based warfare. An effects-based methodology to warfare focuses on enhancing the warfighter's ability to influence an adversary's behavior or decision process by leveraging and integrating other instruments of national power in order to achieve a set of desired effects (Gallinetti, O'Bryan, & Ozolek, 2006). Gallinetti et al. (2006) suggested effects-based operations (EBO) connect "strategic and operational objectives with operational and tactical tasks by identifying desired and undesired effects within the operational environment" (p. I-1). Because the operational environment in cyberspace is contained within a virtual network of information technology infrastructures, creating *effects* that influence decisions in the physical domain is necessary for cyber warfare to have efficacy. Gallinetti et al. defined effects as the "physical and/or behavioral state of a system that results from an action, a set of actions, or another effect" (p. I-3). Therefore, achieving the full set of effects represents the conditions required to accomplish strategic objectives.

Kelly and Kilcullen (2006) noted that EBO is essentially a restatement of classical Soviet deep-operations theory. Simpkin (1987) purported that Soviet theorists Isserson and Tukhachevsky developed deep operations theory in the 1920s and 1930s in which they modeled military force in terms of systems theory. Isserson and Tukhachevsky believed that attacking and neutralizing selected nodes or linking mechanisms within an operating system would disrupt the feedback and control messages essential for system to function (Simpkin, 1987). As a result, according to Kelly and Kilcullen, the supporting components of the enemy's force structure collapse.

Building on deep operations theory, American air strategist, Warden (1994), developed a "concentric rings" model of strategy, which was used during Operation *Desert Storm* in 1990 (Kelly & Kilcullen, 2006). In Warden's approach, the military would target the "Iraqi leadership from the 'inside out' rather than from the 'outside in' by directly attacking its command-and-control structures" (Kelly & Kilcullen, 2006, p. 64). In this approach, warfighters relied heavily on precision strike technologies to succeed by synchronizing physical and electromagnetic forces to achieve the desired effects. In many respects, Kelly and Kilcullen (2006) suggested that Warden developed an "information-age variation of the *Blitzkrieg* technique" (p. 64).

According to Smith (2003), the combination of sophisticated cyber capabilities and techniques coupled with an effects-based approach provides the ability to attack enemy centers of gravity with unprecedented precision and persistence without the need for undesirable physical destruction. This paradigm shift requires a new way to think about warfare. Leaders must shift their mindset from merely placing weapons on target to creating effects designed to shape the behavior of the enemy by integrating and

coordinating actions with an emphasis on non-traditional and non-kinetic methods.

Therefore, cyberspace becomes an obvious and well-suited medium to accomplish EBO.

As a means of engaging adversaries to establish cyberspace control and superiority, Pace (2006a) asserted the military must be able to achieve desired effects in military, intelligence, and business operations.

Cyberspace Operations

Essential for understanding how military officers make response decisions following a cyber attack is a comprehensive description of cyberspace operations (Kuehl, 2009; Pace, 2006a; Wilson, 2007b). Comprised of much more than merely computer network operations, cyberspace operations are the military activities conducted in and through cyberspace that ensure freedom of action within this contested domain (Pace, 2006a). Therefore, in addition to describing computer network operations, this section contains a thorough review of the literature regarding (a) cyber crime and the associated economic impact, (b) cyber terrorism, (c) nation and non-nation state actors, (d) cyber threats and vulnerabilities, and (e) the challenges with attributing malicious cyber activity.

Computer network operations (CNO). In 2008, the Deputy Secretary of Defense defined cyberspace operations as “the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and those activities necessary to operate and defend the Global Information Grid” (England, 2008b, p. 1). Therefore, cyberspace operations fundamentally contain CNO. From a military perspective, Pace (2006a) defined CNO as being “comprised of computer network attack (CNA), computer

network defense (CND), and related computer network exploitation (CNE) enabling operations” (p. GL-1). Within the DoD, the presidentially approved Unified Command Plan (UCP) gives the Commander, U.S. Strategic Command (USSTRATCOM) responsibility for conducting CNO. Under USSTRATCOM’s combatant command authority, the subordinate unified U.S. Cyber Command (USCYBERCOM), in conjunction with the NSA, ensures the persistent operational availability of the GIG using all elements of CNO.

Although integral to cyberspace operations, CNO are also vital to conducting IO. Pace (2006a) defined IO as “the integrated employment of the core capabilities of electronic warfare, *computer network operations*, psychological operations, military deception, and operations security . . . to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own” (p. GL-2). The definition of IO implies CNO create effects that influence decision-making processes. While warfighters use CNO to conduct both IO and cyberspace operations, each mission set is distinctly different and designed to accomplish separate objectives with similar effects. Within military organizations, the differences between IO and cyberspace operations often blur and can be confusing. To help understand the distinction, one should realize cyberspace operations are conducted in or through cyberspace while IO can be conducted in cyberspace or the physical domains.

Computer network attack (CNA). Although cyber warfare takes advantage of each element of CNO, most consider the term cyber attack synonymous with CNA. Specifically, cyber warriors use CNA to “disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks

themselves” (Pace, 2006a). Sophisticated CNA methods use physical means and electronic capabilities to obtain access to an adversary’s network (Tubbs et al., 2002). Physical access, typically gained with the assistance of an insider, empowers the cyber attacker to download or corrupt information, or install software such as a sniffer program to ensure future access (Tubbs et al., 2002). Electronic access, usually obtained through a socially engineered process, allows the cyber attacker to use malicious e-mail attachments to gain control of someone’s computer with administrator privileges (Tubbs et al., 2002).

CNA typically uses a data stream as a virtual weapon during an attack (Wilson, 2007b). For example, CNA use a digital data stream to alter the behavior of a control system, to manipulate the content of a web server, or to shutdown a networked weapon system. Due to the interconnected nature of cyberspace, CNA against networks in one geographic location can have unintended consequences in other networks worldwide. Therefore, CNA against a financial network could adversely affect networks in other critical infrastructures. For this reason, Wilson (2007b) emphasized that second and third order consequences must be clearly understood prior to decision-makers authorizing a CNA against a sovereign nation because a cyber attack has the realistic potential to cause cascading effects capable of causing major disruptions to critical infrastructures.

While sanctioned CNA authorized by leaders at the national level are considered as serious as directing kinetic attacks, professional and amateur hackers conduct malicious activities on the Internet without considering the undesirable ramifications. On a daily basis, hackers post new tools on the Internet for attacking networks, which anyone can download (Barnett, 2002). According to Middleton (1999), the most popular tools

are “password crackers, port scanners, war dialers, general network vulnerability scanners, and intrusion detection systems” (p. 27). In conjunction with these invasive tools, CNA ultimately rely upon flaws in software, enhanced by the access provided by the Internet (Tubbs et al., 2002). Neumann (1995) summarized the various methods of “computer misuse” in Appendix B.

Computer network defense (CND). Computer networks are under constant attack by tools and techniques designed to exploit technical and socially engineered vulnerabilities (Wegener et al., 2003). Therefore, dedicated protection efforts are necessary to defend vital networks and information systems against infiltration from various threat vectors. Accordingly, Pace (2006a) defined CND as “actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks” (p. GL-1). Furthermore, CND measures use information assurance capabilities to detect malicious network intrusions by using threat information derived from intelligence, law enforcement, and military sources in order to alert the appropriate department or agency (Pace, 2006a).

As users create, process, and distribute information, active layered defense measures are essential for protecting the “confidentiality, integrity, availability, authentication, and non-repudiation” (Pace, 2006a, p. F-1) of the associated data. According to Wilson (2007b), CND can take many forms including automatic response actions from passive devices, such as firewalls or data encryption. In addition, Wilson suggested that more aggressive defense measures might include active programmable devices capable of probing an adversary’s network in order to prevent impending attacks via specific information ports, channels, or IP addresses. Wilson concluded that

aggressive defensive measures challenge the existing bounds of current policy and legal authorities associated with the inherent right of self-defense.

Pace (2006a) highlighted that the DoD must employ an information centric, layered defense-in-depth approach to operate and defend military information systems using technical and non-technical practices. These practices should include constant monitoring, accurate detection, detailed reporting, effective prevention, and rapid response to ensure only authorized and legitimate users have access to vital DoD information (Pace, 2006a). Robust CND requires network operations to be integrated with other military activities, including defense support to civil authorities. Because all military personnel operate in cyberspace, training to maintain and improve defense-in-depth measures is essential. Poorly trained personnel might improperly manage and compromise critical networks by inadvertently reducing the security protocols and design features of the GIG, which could easily thwart well-intended CND measures (Pace, 2006a).

Computer network exploitation (CNE). The computer network tools, tactics, techniques, and procedures for conducting CNA are essentially the same as those required to conduct CNE even though the legal authorities are vastly different (Crane, 2002). CNA is considered a traditional military activity conducted under U.S. Code Title 10 (Armed Forces) and CNE is conducted by intelligence agencies under U.S. Code Title 50 (Chapter 36, Foreign Intelligence Surveillance). With this understanding, Pace (2006a) defined CNE as the “enabling operations and intelligence collection methods used to gather data from target or adversary automated information systems or networks” (p. GL-1). The DoD uses network exploitation to gather intelligence and shape the

cyberspace environment as necessary to provide integrated offensive and defensive options. Furthermore, the DoD leverages the authorities and capabilities of those agencies under the Director of National Intelligence to conduct coordinated cyberspace operations across national, geopolitical, and geographic boundaries (Pace, 2006a).

CNE processes provide decision-makers insights into an adversary's use of cyberspace. When CNE techniques are used for military purposes such as "target" validation, the intelligence gathering process is termed "operational preparation of the environment" (OPE). Before a substantial cyber event occurs, Wilson (2007b) noted the military persistently monitors the information battlespace using intelligence, surveillance and reconnaissance (ISR) tactics, techniques, and tools designed to gain information about an adversary's vulnerabilities. As with any other precision weapon system, Tenet (2001) suggested that cyber warfare requires aggressive intelligence capabilities to provide precise and timely information in order to target an adversary's information systems in a clandestine manner without causing unintended or collateral damage. To accomplish CNE objectives, Tenet highlighted that network reconnaissance operations should provide a thorough mapping of target networks in addition to identifying access routes through an adversary's critical information systems.

Cyber crime. Wilson (2008) defined cyber crime as crime that primarily targets computers or computer network systems. For example, Wilson noted, "Cyber crime can involve theft of intellectual property, a violation of patent, trade secret, or copyright laws . . . and includes attacks against computers to disrupt processing or may include espionage to make unauthorized copies of classified data" (p. CRS-4). Unfortunately, cyber criminals can damage a country's economy to such an extent that national security

is ultimately affected. Specifically, Wilson reported that cybersecurity experts believe Russian political protestors hired cyber criminals to conduct cyber attacks against Estonia in April 2007 using a large “botnet” to disrupt their government computer systems.

A fine line exists between cyber crime and cyber war (Knapp & Boulton, 2006). Accordingly, Lewis (2002) found decision-makers at the national level do not fully grasp the technical similarities between cyber espionage and cyber crime, which also tend to blur the line between criminal activity and hostile acts of war. In a congressional report, Wilson (2008) noted that cyber crime is evolving into an organized transnational business that uses cyber criminals with technological skills for rent. Wilson believed that these skills are a commodity to a large variety of sponsors, including nation states. Cyber criminals use sophisticated tools to conduct cyber attacks against financial targets that range from the individual level (identity theft schemes) to the banking industry (credit card fraud). Moreover, cyber criminals target nation states, such as Estonia, where their motives encompass cyber attacks designed for extorting money and inflicting damage on critical infrastructure systems for paid retribution (Wilson, 2008).

Unlike CNO, which is a traditional military activity, the DoD does not have a direct role against cyber crime. Cyber crime is usually handled through domestic channels of authority including the FBI under U.S. Code Title 18 (Crimes and Criminal Procedures) and the DHS under U.S. Code Title 6 (Domestic Security). However, since the line between cyber attack and cyber crime is often overlapping and ill defined, the DoD works closely with other interagency partners to bolster CND efforts worldwide (Knapp & Boulton, 2006; Pace, 2006a). This collaboration is accomplished organizationally through a whole of government approach designed to improve

situational awareness about the health of commercial and government networks by processing, integrating, and sharing information. Organizations such as USCYBERCOM, Defense Cyber Crime Center (DC3), U.S. Computer Emergency Readiness Team (US-CERT), National Security Agency Threat Operations Center (NTOC), Intelligence Community Incident Response Center (IC-IRC), and the National Cyber Investigative Joint Task Force (NCIJTF) facilitate the development of a common operating picture for enhancing the leadership's situational awareness.

Lewis (2002) found that the interplay between cyber crime and cyber warfare forms a highly dynamic and unpredictable relationship. Lewis determined this to be particularly true with the vulnerabilities associated with protecting critical infrastructures. Specifically, vulnerability uncertainty increases, according to Lewis, when societies evolve to a ubiquitous networked environment where daily activities become inherently reliant and ever more dependent on the enticing nature of cyberspace. With this understanding, cyber criminals could apply their skills against supervisory control and data acquisition (SCADA) systems causing disruption to critical infrastructures such as electrical power plants, financial markets, and transportation (e.g., train, airline) deconfliction systems. When cyber criminals hold information systems essential to national security hostage for a ransom, the distinction between cyber crime and cyber warfare distorts even further (Sharma & Gupta, 2002).

Economic impact of cyber crime. Determining the economic impact that cyber crime has on various financial markets is challenging due to the lack of a comprehensive model and inconsistent reporting requirements (Cashell, Jackson, Jickling, & Webel, 2004). However, according to Cashell et al. (2004), several consulting firms recorded

estimates that the “total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general . . . range from \$13 billion (worms and viruses only) to \$226 billion (for all forms of overt attacks)” (p. 2). After studying 43 attacks, involving 38 companies between 1995 and 2000, Campbell, Gordon, Loeb, and Zhou (2003) found attacks that compromised confidential data caused a statistically significant decline in the market value of the respective companies. Furthermore, Campbell et al. determined that e-commerce firms were 5% more likely to have adverse financial effects following a cyber attack.

During the economic impact studies described above, Cashell et al. (2004) divided the cyber attacks into four specific categories: “simple web site defacing, denial of service, theft of credit card information, and theft of other customer information” (p. CRS-5). Of these attack types, credit card information theft was most detrimental. “On the day of the attack, stock prices of affected [credit card] firms lowered by an average of 9.3% and by the third day, the decline reached 15%” (Cashell et al., 2004, p. CRS-5). In addition, Cashell et al. determined a strong relationship between the quantity of credit accounts infiltrated and the stock price decline. For this reason, credit card companies absorb billions of losses each year due to cyber crime in order to prevent the subsequent adverse stock market reaction. Drew (2008) reported that cyber criminals “armed with only a few pieces of personal information such as an address and a social security number . . . caused \$52 billion in identity theft losses in 2002 and affected almost 10 million Americans” (para. 2).

Cyber terrorism. Cyber terrorism is the “premeditated, politically motivated attacks against information, computer systems, computer programs, and data which result

in violence against non-combatant targets by sub-national groups or clandestine agents” (Curran, Concannon, & McKeever, 2008, p. 1). Although no substantial act of cyber terrorism has occurred to date, Curran, Concannon et al. (2008) noted that technology and the Internet have made the possibilities vast. Noting that terrorists usually have limited resources, cyber attacks are appealing because less funding and people are required than necessitated by traditional kinetic attacks. In addition, cyber attacks provide the anonymity and global reach terrorists seek when conducting their acts of intimidation, coercion, and violent extremism.

Just as the lines between cyber warfare and cyber crime are blurred, technology has empowered cyber terrorists to use this ambiguity to their advantage. Wilson (2008) indicated that cyber attacks from politically motivated hackers with the motivation and means to cause serious physical harm, loss of life, and substantial economic impact will continue to increase. With this increase, Lewis (2002) warned that cyber terrorists would eventually use large-scale and well-coordinated cyber attacks to shutdown vital national systems. Cyber terrorists will likely prioritize their attacks against electrical power grids, financial transaction nodes, and transportation systems in order to coerce, intimidate, or terrorize sovereign nations. As critical infrastructures grow more dependent on computer networks for day-to-day business operations, companies supporting these infrastructures become more vulnerable. Lewis viewed this dependency as “a massive electronic Achilles’ heel” (p. 1). When critical infrastructures become vulnerable, cyber terrorists can adversely affect national security with impunity due to the global and covert nature of cyberspace operations.

The vulnerability of critical infrastructures to cyber attack was first highlighted following the 9/11 attacks on the World Trade Centers (Shea, 2003). According to Shea (2003), critical infrastructures are defined in the U.S. PATRIOT Act as:

. . . systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (p. CRS-1)

To date, 18 industry sectors ranging from energy and transportation to telecommunications and banking form the nation's critical infrastructures protected by the PATRIOT Act. As far back as 1997, the Presidential Commission on Critical Infrastructure Protection exposed the vulnerability of the United States to cyber attacks due to the reliance that most industries have on engineered control systems (e.g., SCADA) and digital networks (e.g., Internet; Shea, 2003). The Presidential Commission recognized that the dependency on information systems make critical industries lucrative targets for cyber terrorists through disruption or modification of the data used for operational decisions and control programs (Shea, 2003).

Wilson (2008) noted that cyber terrorists are likely to pay cyber criminals for their tools and techniques to conduct cyber attacks. For example, Wilson reported that cyber criminals have formed agreements and coalitions with drug cartels in South-Central Asia and other host nations where illegal cyber activities fully resource terrorist groups. Furthermore, botnets created by cyber criminals are available for rent to use as cyber weapons against potential economic, political, and military targets. Wilson indicated that these botnets are extremely sophisticated and rival technologies that match the United

States in cyber capability. Therefore, cyber criminals are capable of enabling cyber terrorists to conduct sophisticated cyber attacks without the need to develop costly tools and tactics themselves.

Nation state actors. A revolution in military affairs (RMA), according to Hildreth (2001), is defined as a “significant change in technology taken advantage of by comparable changes in military training, organization, and doctrine” (p. CRS-12). Based on this definition, a RMA is occurring on a global scale due to rapid and metamorphic changes in technological connectivity, capability, and dependency experienced by nation and non-state actors. In recent years, cyber attacks against government and private networks by state-sponsored and non-state actors have increased (Carafano & Weitz, 2008). This trend will likely continue (Matthews, 2008). Therefore, unlike traditional warfare, the ability and anonymity to attack in or through cyberspace tends to equalize the battlespace while providing a large range of actors the opportunity to carry out their political agendas.

Hildreth (2001) reported that the United Kingdom, Germany, France, Russia, and China have CNA and CNE capabilities that rival the United States. According to Matthews (2008), Georgia Tech University published a report that indicated nation-state sponsored cyber attacks will accompany traditional military operations of the future. For example, the country of Georgia in August 2008 experienced cyber attacks from “nationalistic hackers” (Matthews, 2008, p. 5) inside Russia in concert with traditional kinetic warfare. While the Russian government denied conducting these attacks, Russian policy endorses cyber attacks as legitimate military operations. Similar large-scale cyber attacks against Estonia in May 2007, originating from inside Russia, targeted banks,

government websites, telecommunication networks, and media companies, finally resulted in Estonia blocking all foreign Internet traffic (Carafano & Weitz, 2008).

Hildreth asserted Russia ranks cyber warfare second only to nuclear warfare.

Furthermore, Hildreth emphasized that Russia considers computer viruses, botnets, and other cyber weapons are effective force multipliers, capable of complimenting traditional warfare.

According to a DoD report released in 2007, China presents a considerable threat to U.S. cybersecurity (Matthews, 2008). Specifically, many cyber attacks against military networks have been attributed to Chinese sources. Matthews (2008) reported that Heron, former chief scientist and security expert for McAfee, believes Chinese cyber attacks are more sophisticated than would be expected by typical hackers. Furthermore, Heron asserted that the coordinated cyber attacks currently being conducted by the Chinese are programmatic and threaten more than the U.S. military networks (Matthews, 2008).

Senior defense analysts, as reported by Carafano and Weitz (2008), believe that China has incorporated the systematic development of information warfare capabilities into their overall national security strategy in order to “achieve ‘electromagnetic dominance’ over the United States and other potential competitors” (p. 2). Hildreth (2001) noted the Chinese theory of cyber warfare incorporates the modern People’s War concept and the ancient 36 Stratagems, which form the basis of their military doctrine. To the Chinese, cyber warfare, according to Hildreth, is a “transformation from the mechanized warfare of the industrial age to . . . a war of decisions and control, a war of knowledge, and a war of intellect” (p. CRS-12).

Non-Nation state actors. “The rise of al Qaeda has reminded the world of the power of the non-state actor, so too has the rise of the individual hacker” (Stratfor, 2008a, para. 3). Non-state actors conduct malicious cyber activities that are not directly sanctioned, authorized, or affiliated with a sovereign nation state. Non-state cyber activities can take the form of cyber crime, terrorism, or warfare. According to Wilson (2008), non-state cyber specialists are usually “hackers” or “crackers” who rent their skills and capabilities to nation states, terrorists, and criminal organizations. Wilson warned that new and highly effective cyber tools allow hackers to perform cyber warfare services for nation states by providing an additional level of anonymity while conducting sophisticated attacks through the Internet. For example, many experts claim that the cyber attacks against Estonia in 2007 and Georgia in 2008 used non-nation sanctioned state “hacktivists” inside of Russia to execute these operations (Wilson, 2008).

Lichstein (1963) first used the term “hackers” in the Massachusetts Institute of Technology’s (MIT) weekly student paper, *The Tech*. In this article, Lichstein wrote, “The *hackers* have accomplished such things as tying up all the tie-lines between Harvard and MIT, or making long-distance calls by charging them to a local radar installation” (p. 1). Since then, according to McFedries (2004), the term “hackers” has conveyed a negatively construed image of individuals who use their expert computer skills for gaining unauthorized access to computer and telecommunication networks.

However, McFedries (2004) noted that purists in the computer industry prefer the term “cracker” when describing a digital miscreant. Disgruntled hackers coined the term “cracker” in 1985 angered by the journalistic misuse of the term hacker (Schell & Martin, 2004). Curran, Breslin, McLaughlin, and Tracey (2008) defined cracker as someone who

individually benefits by hacking into a computer network system. Stratfor (2008b) added that crackers frequently bypass or ignore copyright laws on digital media, thus making software programs and applications more readily available to the hacker community at large.

Stratfor (2008b) classified hackers into two broad categories, “black hats” and “white hats.” Black hat (or dark side) hackers conduct malicious cyber activity for the purposes of crime or terrorism (Stratfor, 2008a). White hat hackers (or sneakers) conduct authorized cyber activities for the purposes of penetrating computer systems and networks to determine vulnerabilities and intrusion flaws (Stratfor, 2008a). Companies hire white hats to penetrate their networks in order to make their information systems more secure. Comprised of highly trained personnel called “red teams,” military white hats determine GIG vulnerabilities to ensure command and control networks, weapon systems, as well as communication systems are secure.

Cyber threats. The first reported case of hacking, according to Macz (2002), occurred in 1878 when teenage boys hired as telephone switchboard operators mischievously misdirected phone calls and eavesdropped on conversations. Nearly 100 years later, students at MIT conducted the first official “hack” when they modified their train sets to operate differently from originally designed. These hackers quickly realized their newfound skills could be applied to gaining access to the new computer systems installed on the MIT campus during the 1960s (Macz, 2002). Early hackers did not view their actions as exploiting system vulnerabilities. Instead, hackers were thrill seekers who enjoyed covertly replacing original programs with customized code designed to be more elegant, innovative, and functional.

Cyber threats and vulnerabilities are often used interchangeably; however, the terms are not equivalent. Alexander (2006) defined a cyber threat as “any circumstance or event with the potential to affect an information system adversely through unauthorized access, destruction, disclosure, modification of data, and/or denial of service” (p. 61). Fry (2008) defined cyber vulnerabilities as “weaknesses in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system” (p. 585).

Lewis (2002) found that much of the early work conducted on researching cyber threats focused on hackers, terrorists, and foreign intelligence agencies infiltrating and taking over a computer network system from a remote location as a means of disrupting a nation’s critical infrastructures. However, Lewis’ reported evidence has not supported this premise. Lewis’ assertion held true until 2007 when Russian hacktivists attacked Estonia with a massive distributed denial of service attack that successfully shutdown several critical information systems (Lewis, 2007). To understand the potential vulnerability a cyber threat poses to a critical infrastructure, each target infrastructure would require a comprehensive assessment of redundancy, normal failure rates, public accessibility to critical control functions, the designed level of human interface, and how closely critical operations are monitored (Lewis, 2007).

Pace (2006a) determined that cyber threats usually fit into six different categories: traditional, irregular, catastrophic, disruptive, natural, and accidental. Traditional threats are associated with the employment of military forces and capabilities by nation states in “well-understood forms of military conflict . . . that enable air, land, maritime, and space operations” (p. C-1). Irregular threats arise when non-state actors use cyber capabilities

as an unconventional, asymmetric means to counter traditional warfare methods. For example, terrorists could mask or enhance a kinetic attack by conducting cyberspace operations against financial and industrial sectors. Furthermore, Pace asserted, “Irregular threats from criminal elements and advocates of radical political agendas seek to use cyberspace for their own ends to challenge government, corporate, or societal interests” (p. C-1).

Catastrophic threats are associated with the acquisition, possession, and use of WMD. Within cyberspace, WMD-like effects are possible using large botnets or directed energy devices against networked control systems or against key nodes of critical infrastructures where cascading effects could cause devastating consequences nationally and globally (Pace, 2006a). Although Lewis (2002) reported that the employment of cyber weapons on a WMD scale is unlikely, the threat of such use forms the basis for developing a national cyber deterrence policy (Welch, 2007).

Disruptive threats, according to Pace (2006a), exist as breakthrough technologies with the potential to negate or minimize the advantage the United States has within a warfighting domain. The fear of disruptive threats necessitates increased research and development on a national laboratory level in addition to building key partnerships with the industrial technology sector to ensure the United States maintains the appropriate level of readiness (Pace, 2006a). Because the DoD depends primarily on technology developed by private industry, fostering trust relationships is essential to sharing threat information across the DIB.

Natural threats resulting from floods, hurricanes, solar flares, lightening, and tornadoes can disrupt cyberspace operations. Furthermore, natural disasters provide

opportunity for adversaries to conduct cyber attacks that exploit computer systems that are already in a degraded condition (Pace, 2006a). Accidental threats, such as cutting a fiber optic cable with a backhoe or a trawler dragging an undersea cable can cause major disruptions to cyberspace. Accidental threats are more impacting to countries with restricted bandwidth due to their limited information technology infrastructures.

Cyber vulnerabilities. According to Ahamad et al. (2008), data are the most vulnerable cyber asset. Ahamad et al. predicted that data would continue to be the primary motive for conducting cyber attacks against information and communication technologies for years to come. Data in the form of transactions play a substantial role in cyberspace commerce. VeriSign, a company that provides secure transactions, reported ecommerce resulted in more than \$14 billion in U.S. sales resulting from over one billion Internet users worldwide (Pace, 2006a). Data become vulnerable from several mechanisms including hardware, software, operating procedures, and personnel.

By design, the architecture of cyberspace is inherently vulnerable to malicious activity (Pace, 2006a). Insecure network protocols and exploitable firmware within routers combined with the extremely large number of connection points make securing cyberspace nearly impossible. In addition, the nature of cyberspace enables military operations intended to be local in scope to have unintended effects globally.

Furthermore, the physical protection associated with the Internet's infrastructure is lacking. According to Pace (2006a), insufficient protective measures and poor physical security for cyberspace components such as cables, facilities, sites, structures, and equipment provide an easy target for adversaries to disrupt cyberspace operations.

Technical vulnerabilities are intrinsically problematic for cyberspace. Pace (2006a) found that vulnerabilities in operating systems, software applications, and controlled interfaces can allow threat actors to gain unauthorized access to information systems and data, and enable them to disrupt system functionality at their discretion. Threat actors proficient in software programming, signaling command and control, protocol architectures, or encryption may inject malicious data into software, firmware, hardware, and encryption mechanisms to render the data useless or crack encryption for data collection (Pace, 2006a).

The nature of cyberspace necessitates a codependency between numerous organizations and industries for technology innovation, development, and implementation (Ahamad et al., 2008). This dependency creates a vulnerable environment where one malicious actor can cause insidious damage. For example, operating with international partners, agencies, and allies in cyberspace introduces substantial vulnerabilities especially if cyberspace security is not a unilateral priority or if security is not consistently applied.

Outsourcing can cause additional vulnerabilities (Pace, 2006a). When commercial and military technological requirements are outsourced, exploitation could occur anywhere within the supply chain manufacturing and distribution processes. Throughout a product's technology life cycle, adversaries can discover or cause vulnerabilities in commercial off-the-shelf software and hardware installed on DoD systems and networks. Ahamad et al. (2008) warned that using open source technologies exacerbates this problem. Pace (2006a) asserted that potential threat actors could use

publicly available information and employ data mining methods to focus intelligence collection efforts and plan attacks against DoD networks.

The lack of formal training and education programs can create substantial vulnerabilities (Ahamad et al., 2008). Military personnel, including senior leaders, commanders, cyberspace operators, and ordinary users, all require thorough training for effective cyberspace operations (Pace, 2006a). Without a continuous training program, users lose awareness of adversary techniques such as socially engineered e-mails and websites designed to gain access to networks, systems, and information. Therefore, Pace (2006a) considered user training to be an integral part of an organization's defense-in-depth measures. Poorly trained personnel can carelessly or incorrectly install, maintain, or secure systems; mishandle passwords; or improperly check for malicious software.

Attribution challenges. Inherent to any deterrence theory, including cyber deterrence, is the concept of *attribution* (Phillips, 2007; Taipale, 2009). Attribution is the ability to detect the source of an attack and assign credit to a specific adversary with a satisfactory level of certainty (Kugler, 2009; Wheeler & Larsen, 2007). In cyberspace, Saunders and Levis (2007) suggested the redundancy properties and design of Internet protocols promote anonymity, which adversely affect the ability to trace the source of a cyber attack and thus, attribute the attack to a malicious perpetrator. Therefore, enhanced technologies and capabilities for improving attribution are “required for nuclear, chemical, biological, radiological, and explosive weapons as well as attacks on space systems and computer networks” (Cartwright et al., 2006, p. 31).

In the *National Strategy to Secure Cyberspace*, Bush (2003) emphasized that deterring cyber threats is a goal of the United States (Callaghan & Kaufmann, 2008).

Understanding the challenges associated with accurate attribution, Bush (2003) stated, “Our strategy cannot be to eliminate all vulnerabilities or to deter all threats” (pp. 27-28). Furthermore, Bush noted, “The speed and anonymity of cyber attacks make distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all” (p. viii).

Wilson (2007b) described the accurate and timely identification of the attacker after a CNA as extremely challenging. This challenge adds uncertainty and dramatically affects response action decisions. The attribution problem is arguably the single largest factor that differentiates attacks in cyberspace from attacks in other physical domains. To this point, Gourley (2008) asserted, “The primary challenge [for cyber warfare] is one of attribution of attack” (para. 5). When attribution challenges combine with the immaturity of cyber warfare doctrine, warfighters face immense decision-making uncertainty in determining the appropriate response action (Kugler, 2009).

Schmitt (2002) warned that attribution is also a legal concern. Specifically, Schmitt noted the laws applicable to international armed conflict require defensive response actions be attributable to a particular nation state or adversarial entity. Recognizing the complexity of making lawful response decisions following a cyber attack from different actors (e.g., sovereign states, terrorists, criminals, and spies), Wingfield, Michael, and Wijesekera (2005) proposed a framework to facilitate the systematic portions of the decision-making process by minimizing the need for human intervention to only those legal decisions that require human judgment and official accountability. A more thorough coverage of the legal aspects associated with cyber attacks is presented later in chapter 2.

Decision-Making under Risk, Uncertainty, and Ignorance

As responsible decision-makers, military leaders are compelled to make well-informed and effective decisions. Decisions are the cognitive products that result from judgment by making up one's mind after due consideration (The American Heritage Dictionary, 2006). According to military doctrine, a decision is "an estimate of the situation, a clear and concise statement of the line of action intended to be followed by the commander as the one most favorable to the successful accomplishment of the assigned mission" (Fry, 2008, p. 148). Given that terms such as *judgment*, *estimate*, and *favorable* appear in the definitions above, decision-making, in general, is not an exact science where outcomes are known with deterministic precision. Instead, decision-making is a complex process occurring along a spectrum of certainty where probability distributions, experience, intuition, rationality, risk acceptance, and guessing factor into the decision calculus (Vowell, 2004).

In the germinal work on risk and uncertainty, Knight (1921) proposed that decision-making occurred along a "continuum of the known, the unknown, and the unknowable" (Kleindorfer, 2008, p. 2). Knight's work, conducted primarily in an economic context to explain taking chances when making financial decisions, made the first distinction between certainty and non-certainty (Hansson, 2005). Knight defined the term "risk," frequently used in everyday speech within financial circles, as "a quantity susceptible of measurement" or a "measurable uncertainty" (pp. 19-20). With this in mind, Knight defined "uncertainty" as a "non-quantitative" (p. 20) state of mind. Knight asserted the phenomenon of uncertainty accounted for the differences between actual and theoretical competition, which was lacking in economic theories of the time.

In their influential book on game and decision theory, Luce and Raiffa (1957) refined the distinction between certainty and non-certainty in an effort to link accepted terminology with the mathematics of utility theory. In their work, Luce and Raiffa described *certainty* (the known) as the condition in which an action leads to a known outcome, prospect, or alternative. Luce and Raiffa divided non-certainty into two categories, *risk* (i.e., the unknown) and *uncertainty* (i.e., the unknowable; Hansson, 2005). Therefore, decisions under risk are based on alternatives (or states of nature) with known probabilities as opposed to decisions under uncertainty, which are based on alternatives with unknown probabilities. When outcome probabilities are approximate or fall within a certain range, this situation commonly is referred to as *uncertainty* as well (Hansson, 2005). When this convention is adopted, the more strict definition of uncertainty, defined by Luce and Raiffa, is referred to as *ignorance* (Hansson, 2005).

Other than academic scenarios, decisions are seldom made under certainty because complete knowledge regarding the possible outcomes is not likely (Hansson, 2005; Kleindorfer, 2008; Knight, 1921). This assertion holds true for military operations, including cyber warfare decisions in which extraordinary complexity and unintended effects are prevalent (Butler et al., 2005; Nicholson, 2005; Schultz, 1997; Vowell, 2004). At best, warfare decisions are made under risk; however, most decisions commanders encounter are made under uncertainty because of what Clausewitz described as the “fog of war” (Cowan, 1996; Nicholson, 2005; Vowell, 2004). Even with today’s most sophisticated surveillance and reconnaissance systems providing real time situation awareness in support of a common operating picture of the battlefield, the complexity of modern warfare precludes commanders from exercising *coup d’oeil* (i.e., an “inner light”

to see truth through the fog of war; Cowan, 1996; McCauley-Bell & Freeman, 1997; Vowell, 2004).

According to Nicholson (2005), the “complexities of war will always create uncertainty and friction because war involves the human dimension, the enemy, and technology” (p. 57). Although innovative technologies will continue to improve the science of military operations, Nicholson maintained commanders must still master the art of warfare in order to make effective decisions. Battle command is the result of professional competence, relentless practice, and measured judgment (U.S. Army Field Manual [FM] 3-0, 2008). Mastering the art of battle command requires situation awareness, decision-making processes, and leadership skills refined from experience, education, and expertise (FM 3-0, 2008). Given these skills, the commander still requires relevant information to make decisions along with a process of transforming that information into knowledge. A sound decision-making process coupled with Clausewitz’s “qualities of a military genius” (i.e., courage, intelligence, coup d’oeil, and resolve) is the formula for a gifted warrior (Nicholson, 2005).

The Military Decision-Making Process (MDMP)

The MDMP is a rigorous, deliberate, and time-consuming procedure, honed over the last two centuries, and designed to help Joint Force Commanders by integrating “intuition with analysis, task with purpose, plans with operations, and the present with the future” (Paparone, 2001, p. 45). The MDMP emerged and began taking form in late 19th century as an outcome of the first recognized *Generalstab* (general staff) under the leadership of Prussian General Helmuth von Moltke (Cowan, 1996; Paparone, 2001). Following several decisive defeats from Napoleon, the Prussian army recognized a need

to train their officers how to make effective military decisions using a repeatable and reliable process (Cowan, 1996).

The U.S. Army adopted the MDMP in the 20th century (Cowan, 1996). As war complexity increased, the U.S. Army refined the MDMP several times in order to accommodate best practices while improving the adaptability of the process based on varying staff sizes and decision timeframes (Cowan, 1996; Paparone, 2001). According to the U.S. Army Field Manual [FM] 5-0 (2005), the MDMP is a planning tool that provides a systematic process for evaluating a mission, creating courses of action (COAs), comparing the COAs against success criteria, and selecting the optimum COA in order to produce a plan or order. Therefore, the MDMP facilitates decision-making by balancing the commander's intuition with the general staff's analytical planning rigor. In this context, decision-making is defined as "selecting a course of action as the one most favorable to accomplish the mission" (FM 5-0, 2005, p. I-6).

Warfare commanders must make challenging decisions in an environment of substantial uncertainty, unpredictability, and continuous change. Given time, commanders make deliberate decisions using the MDMP and their staffs to create a fully developed course of action. Deliberate decisions rely more heavily on the analytic decision-making process. When time is of the essence and the MDMP cannot be completed in its entirety, the commander must rely more on intuitive decision-making. Analytic decision-making approaches a problem systematically and methodically by generating several potential solutions; analyzing and comparing the possible solutions using weighted criteria; and selecting the best solution based on the situation.

Intuitive decision-making involves the “act of reaching a conclusion that emphasizes pattern recognition based on knowledge, judgment, experience, education, intelligence, boldness, perception, and character” (FM 5-0, 2005, p. I-6). Intuitive decision-making emphasizes assessing the situation versus comparing multiple options. Rarely are the two approaches mutually exclusive. Despite inevitable uncertainty and ambiguity, successful commanders exhibit sound judgment when they are capable of effectively integrating experienced-based intuition with rigorous analytical expertise.

Decision Theory

Based on the review of the literature strategy described at the beginning of chapter 2 and illustrated in Figure 1, a thorough treatment of cyber warfare and decision-making theory including the MDMP was necessary prior to discussing applicable decision theories. The review of the literature strategy was developed in this manner because the decision theories that follow were researched within the context of their applicability to cyber warfare decision-making where appropriate (DeRouen, 2000; Frank, 1975; Mathers, 2007; Mintz, 1993; Nincic, 1997). In this section, decision theory is described from general background material to specific theories that support use of force response decisions. Included in this section is a comprehensive discussion of compensatory and noncompensatory decision strategies and associated theories.

Decision theory background. Decision theories can be categorized into three main groups: normative, behavioral, and naturalistic (Shao, Lye, Rundle-Thiele, & Fausnaugh, 2003). With origins in game and economic theory, normative decision theory (Bernoulli, 1954; von Neumann & Morgenstern, 1944) is used to order or quantify the complexity of a decision by assuming the decision-maker is rational (Edwards, 1954;

Simon, 1955). With normative decision theory, rational choices are made by following a set of axioms in which consequences are assigned values used to compute the expected utility of possible outcomes (Hastie & Dawes, 2001). In this static model, the rational decision-maker chooses a single outcome based on the largest expected utility among several COAs.

Behavioral decision theory (Edwards, 1961) extends normative theory by adding a descriptive dimension (Einhorn & Hogarth, 1981; Slovic, Fischhoff, & Lichtenstein, 1977). The incorporation of descriptive decision theory includes the study of beliefs, values, judgment, inference, and choice (Slovic et al., 1977). Behavioral decision theorists found that decision preferences and strategies vary across descriptions and are contingent on the decision-maker and situation (Shao et al., 2003). Therefore, using behavioral decision theory allows multiple strategies to be constructed when assessing probabilities during the decision-making process (Tversky & Kahneman, 1974). Shao et al. (2003) asserted this constructive view of decision-making forms the primary distinction between behavioral and normative decision theory.

Naturalistic decision theory was introduced in 1989 following a conference designed to study how decisions were made based on experience in natural settings (Klein, Orasanu, Calderwood, & Zsombok, 1993). Zsombok and Klein (1997) provided the following definition:

Naturalistic decision-making theory describes how experienced people, working as individuals or groups in dynamic, uncertain, and often fast-paced environments, identify and assess their situation, make decisions and take actions

whose consequences are meaningful to them and to the larger organization in which they operate. (p. 5)

Founded on real world research, naturalistic decision theory is used to depict decision-making as a sequence of activities and incorporates multiphase models in which different decision strategies are used to evaluate ambiguous circumstances (Shao et al., 2003).

Therefore, naturalistic decision models are not limited to a single decision process that derives a final choice or outcome, as is the case for single-phase normative or behavioral decision models.

Decision strategies. Decision strategies are a function of compensatory and noncompensatory decision processes in which decisions are made based on alternatives, attributes, or both (Shao et al., 2003). The characteristics of many decision models are summarized in Appendix C. With compensatory strategies, leaders make decisions by weighing the value of attributes in order to determine the possible alternatives (Keller & Yang, 2008). Therefore, compensatory strategies require meaningful amounts of information in order to evaluate and assess the tradeoffs between high and low value attributes (Shao et al., 2003).

Noncompensatory strategies do not require decision-makers to make trade-offs between attributes associated with the decision task. Rather, noncompensatory strategies involve making decisions based on if an attribute meets a predetermined threshold (Shao et al., 2003). Keller and Yang (2008) noted that leaders make noncompensatory decisions by rejecting alternatives based on unacceptable dimensions. Specifically, high value attributes cannot compensate for low value attributes during the decision process.

Decision strategies typically involve analyzing alternatives and attributes.

Alternative-based strategies require the leader to view all the attributes associated with an alternative before considering the next course of action. With attribute-based strategies, leaders identify and compare individual attributes between several alternatives prior to selecting and evaluating the next attribute. Experimental evidence, according to Keller and Yang (2008), supports the supposition that most decisions are two-stage processes. The first stage is a dimension-based process (compensatory or noncompensatory) with an alternative-based process (rational or behavior) in stage two (Mintz, 2004).

Compensatory decision theory. Bueno de Mesquita and Lalman (1992)

suggested, “Nations are led by rational, forward-looking, expected-utility-maximizing leaders who make [use of force] decisions in a holistic and compensatory (additive) fashion” (p. 751). The decisions these leaders make are a function of the relative perception of how adversaries will respond to strategic decisions based on their respective value and belief systems (Bueno de Mesquita & Lalman, 1992). Using a cost-benefit analysis, decision-makers evaluate each course of action to obtain the optimal expected utility with the minimum operational risk (Bueno de Mesquita, 1984). Although the expected utility theory approach is the primary decision paradigm when considering international issues, Mintz (2004) argued that the theory has limitations. Specifically, cognitive and behavioral theorists have found analytical decision-making strategies, such as expected utility theory, require “extensive processing time, cognitive effort, concentration, and skills that in many cases are not available, especially under time pressures and rapidly changing conditions [such as cyber warfare]” (Mintz, 1993, p. 596).

According to Redd (2002), expected utility and cybernetic decision-making theories are based on the assumption that leaders use compensatory decision rules. While compensatory models often are used to explain nation state decisions to use force, Redd suggested these models do not completely characterize the motivational basis associated with political viability. Specifically, Redd asserted leaders would unlikely choose a use of force alternative (outside of responding to an act of war) if that decision would hurt them politically, regardless how attractive the other attributes of that decision might seem. Mintz (1995) found that many experimental studies designed to investigate how decisions were made found decision-makers typically do not employ holistic or purely compensatory processes during complex decision scenarios.

Noncompensatory decision theory. Compensatory models are linear, additive models in which the dimensions for each decision alternative are associated with a specific value and combined algebraically to produce an overall characteristic summation (Mintz, 1993). As an example of compensatory models, a higher valued military or economic dimension can “compensate” for a lower valued political or diplomatic dimension because the leader makes a decision to use force based on the *overall* score (Mintz, 1993). On the other hand, noncompensatory decision-making models are not based on a compensatory (or additive) decision calculus process. Specifically, for each alternative in a choice situation, a large value on a desirable dimension cannot compensate for (or negate) an unacceptable dimensional element. Therefore, the decision-maker would eliminate that alternative and begin considering the next one using the same non-compensatory process (Mintz, 1993).

Noncompensatory models capture the non-holistic nature of decision-making by focusing on an extremely limited set of dimensions and alternatives. Instead of applying a comprehensive set of decision rules in which every dimension of each alternative is analytically assessed and compared, the decision-maker relies on heuristics to eliminate undesirable alternatives using rejection attributes derived from personal experience, historical precedence, and current political climate (Mintz, 1993). Whereas the expected utility and cybernetic use of force models are alternative-based, noncompensatory models are dimensional or attribute-based (Mintz, 1993).

In this context, a dimension is an organizing theme for related information and variables (Ostrom & Job, 1986). In the compensatory linear model, the values of dimensions are summed as utility scores to form an alternative. In contrast, the value of a *critical* dimension is evaluated against a threshold level in a noncompensatory model. If a critical dimension's value is less than the predetermined threshold, then the alternative is no longer considered a viable option (Keller & Yang, 2008; Mintz, 1993). For noncompensatory decisions, Mintz (1995) proposed that certain dimensions dictate the decision-making process in such a way that precludes the requirement to analyze other dimensions when making a complex choice. Therefore, according to the noncompensatory principle, if an alternative is unacceptable along a particular political dimension, then that alternative must be rejected because it cannot be compensated or counteracted by another attractive or highly valued dimension (Mintz, 1995).

Poliheuristic decision theory. The related characteristics of cognitive and rational decision-making theories are leveraged by poliheuristic theory (Mintz, 2004). Poliheuristic choice theory is based on a two-stage decision process. In the first step,

according to DeRouen and Sprecher (2004), alternatives are eliminated by a noncompensatory analysis using simplified heuristics (i.e., cognitive shortcuts). In the second step, the remaining alternatives are evaluated by employing a rational or compensatory means by seeking to minimize risks and maximize benefits (Mintz, 2004).

Examples of the noncompensatory heuristics that inform the elimination of options include restraining the use of force based on political or diplomatic considerations (Mintz, 2004). With poliheuristic theory, the results of the decision-making opportunity are highlighted by explaining why and how leaders make decisions (Mintz, 2005). According to Mintz (2004), poliheuristic theory has been applied to a myriad of decision-making situations including the use of force (Mintz, 1993), diversionary use of force (DeRouen, 2000; Nincic, 1997), initial crisis reaction (DeRouen & Sprecher, 2004), and the level of force used in a crisis (Redd, 2002).

Cybernetic decision theory. Simon (1959) laid the groundwork underpinning cybernetic decision theory in early research on bounded rationality. Steinbruner (1974) refined the cybernetic model to explain how individuals make decisions in environments surrounded by complexity and uncertainty. Cybernetic decision-making is founded on the minimization of uncertainty through information feedback loops. Ostrom and Job (1986) applied the cybernetic model to presidential decisions to authorize the use of force within a political context. An assumption of the cybernetic model is the leader is not able to observe, consider, and evaluate all available stimuli generated from the complex decisional environment; rather, decision-making should be viewed as a repetitive process that occurs using reduced (or incomplete) information with limited (or imperfect) cognitive capabilities (Waterman, 1997).

A cybernetic decision-maker is one who makes the decision to use force based on a thorough assessment of a select number of environmental stimuli, variables, and constraints (Waterman, 1997). Consequently, cybernetic decision processes are less comprehensive since the decision-maker only considers a subset of the possible alternatives and dimensions (Mintz, 1993). With bounded rational models such as the cybernetic decision model (Ostrom & Job, 1986), leaders operate under constraints and only consider a limited subset of alternatives that “satisfice” certain criterion (Mintz, 1993, 1995). While prominent in the 1980s as the primary option to the rational analytic approach, Sylvan and Majeski (2006) asserted cybernetic decision theory should be revived as a valid mechanism for making foreign policy, national security, and use of force decisions.

Utility theory. The term “utility” first appeared in reference to risky monetary ventures as early as 1728 when Cramer wrote, “In practice, people with common sense evaluate money in proportion to the utility they can obtain from it” (Fishburn, 1989, p. 127). A decade later, Bernoulli furthered this idea in 1738 with the assertion, “The *value* of an item must *not* be based on its *price*, but rather on the *utility* it yields” (Fishburn, 1989, p. 127). Bentham (1823) formalized the concept of utility by publishing, “Utility is that property in any object whereby it tends to produce benefit, advantage, pleasure, good, or happiness . . . or . . . to prevent the happening of mischief, pain, evil, or unhappiness” (pp. 3-4). Over the next 100 years, economists contended with different notions of utility including desirability and wantability until von Neumann and Morgenstern published their germinal work on utility theory in 1944.

Utility theories vary based on whether the decision-maker is making choices under certainty, risk, or uncertainty. Luce and Raiffa (1957) defined *certainty* as the condition where “each action is known to lead invariably to a specific outcome, prospect, or alternative” (p. 13). On the other hand, Luce and Raiffa considered decisions under *risk* occur if an “action leads to one of a set of possible specific outcomes [with] each outcome occurring with a known probability” (p. 13). Last, Luce and Raiffa asserted that *uncertainty* results when an “action has as its consequence a set of possible specific outcomes, but where the probabilities of these outcomes are completely unknown or are not even meaningful” (p. 13).

With expected utility theory, according to Mongin (1997), the decision-maker chooses between risky and uncertain alternatives by evaluating the expected utility totals (i.e., the algebraic sum of individual utility values weighted by the respective probabilities). Categorized as normative and prescriptive, utility theory has specific limitations despite historically being a highly useful decision theory (Mongin, 1997). These limitations led to the development of two distinct versions. Specifically, subjective expected utility theory resulted from the study of *uncertainty* and von Neumann-Morgenstern theory from the consideration of *risk* (Mongin, 1997). Known for the “axiomatization” of Bernoulli’s utility model among their noteworthy contributions to game theory, von Neumann and Morgenstern, given a constrained number of possible states, proved that a normative choice relationship could always be expressed as an expected utility (Mongin, 1997).

Prospect theory. As described above, expected utility theory has been a predominate theory for making decisions under risk since first proposed by Bernoulli in

1738 (Kahneman & Tversky, 1979). As a normative, rational model of choice, expected utility theory is applied frequently as a descriptive model of economic and foreign policy decision-making (Kahneman & Tversky, 1979; Redd, 2002). However, based on the required axiomatic constraints, Kahneman and Tversky (1979) found expected utility theory to be an inadequate descriptive model for making choices under risk. Therefore, Kahneman and Tversky developed an alternative model called prospect theory.

As the primary alternative to expected utility theory, Kahneman and Tversky (1979) found that human behavior must be considered when assessing possible choices. Accordingly, Levy (1992) found that prospect theory is founded on the premise that decision-makers evaluate outcomes as a differential from a frame of reference rather than with respect to an arbitrary asset level. Levy noted this reference point is a critical parameter. Furthermore, with prospect theory, individuals consider losses disproportionately more detrimental than comparable gains making them risk-averse with regard to gains and risk-acceptant with regard to losses (Levy, 1992).

Levy's (1992) observations are consistent with Kahneman and Tversky's (1979) assertion that decision-makers undervalue lower probability outcomes when compared to more certain outcomes. This tendency is called the *certainty effect*. Moreover, Kahneman and Tversky found that decision-makers normally reject common elements shared by all prospects under consideration. This tendency is called the *isolation effect*. With prospect theory, unlike expected utility theory, the decision-maker assesses the gain and loss functions individually using decisional weights rather than evaluating final summative values using probabilities.

Due to these properties, Kahneman and Tversky (1979) suggested prospect theory is useful for insurance and gambling decisions. Additionally, Schultz (1997) found that prospect theory can be effectively used when making warfare decisions as well. To understand this assertion, reviewing Clausewitz's (1873) thoughts on the uncertainty of warfare is helpful:

The subjective nature of war and the means by which war has to be fought . . . looks more than ever like a gamble In short, absolute, so-called mathematical, factors never find a firm basis in military calculations. From the very start, there is interplay of possibilities, probabilities, good luck and bad that weaves its way throughout the length and breadth of the tapestry. In the whole range of human activities, war most closely resembles a game of cards. (p. 10)

Although unable to predict the alternative a leader will select, prospect theory can facilitate exposing bias toward a risky or overcautious solution, which might assist in shaping the COAs developed or considered (Schultz, 1997). Using prospect theory, commanders may better understand their personal limitations with respect to accepting too much or too little risk.

Regret theory. Prior to Loomes and Sugden's (1982) germinal work on regret theory, the main body of knowledge on decision theory was built primarily upon von Neumann and Morgenstern's (1944) expected utility theory axioms of rational behavior. However, Loomes and Sugden found that many leaders make decisions that systematically violate these axioms. Building on Kahneman and Tversky's (1979) prospect theory, Loomes and Sugden's regret theory is simpler and more closely aligned with decisional intuition. Loomes and Sugden asserted that their alternative theory

accounts for one's capacity to expect or foresee thoughts of regret, rejoicing, and other choice-based emotions that traditional, normative theory of rational behavior fails to predict. Although the characterization of behavior with regret theory contradicts the axioms of expected utility theory, Loomes and Sugden maintained their theory is rational and has normative implications.

The incorporation of emotions such as regret and disappointment into decision theory research is becoming more popular (Connolly & Zeelenberg, 2002; Pfister & Böhm, 2008). Of the emotions that have been studied, regret has received the most attention (Connolly & Zeelenberg, 2002). Regret, according to Zeelenberg (1999), is a negatively perceived emotion that occurs once one realizes that the existing situation would be better had a different decision been made. After making a decision under uncertainty, the experience of post-decisional regret is linked inextricably to the knowledge of the outcomes associated with the rejected alternatives (Zeelenberg, 1999). By explicitly incorporating regret, expected utility theory becomes a more comprehensive and persuasive model for describing and predicting behavioral decision-making factors (Bell, 1982).

Böhm and Brun (2008) suggested that emotions are an integral component of weighing judgments, perceiving risk, and making decisions. In addition, Böhm and Brun noted that intuition has become an increasingly popular topic in decision-making research. Incorporating emotions and intuition into decision theory has been essential to the evolution of dual-process models and heuristic/bias approaches (Böhm & Brun, 2008). Therefore, two distinct modes of decision-making have evolved. One mode corresponds to the traditional, rational, and deliberate approach of normative decision

theory. The other mode accounts for feelings, emotional judgments, and intuition. The inclusion of emotion into decision-making improves information flow, evaluation speed under time constraints, situational relevance, as well as social and moral commitment to the final decision (Pfister & Böhm, 2008).

Game theory. In 1921, the French mathematician Borel, building on the work of Zermelo, published several papers that formed the origins of modern game theory (International Federation of Operational Research Societies [IFORS], 2006; Kelley, 2003; Luce & Raiffa, 1957). However, Borel was never able to prove the minimax theorem (Kelly, 2003; Luce & Raiffa, 1957). Known as the fundamental theorem of game theory, Waldegrave proposed the minimax theorem in 1713 to describe the existence of a set of strategic approaches used by the players in a competitive game in which none of the players regrets their choice of strategy after the game is finished (Kelley, 2003).

Luce and Raiffa (1957) reported that von Neumann's paper published in 1928 is attributed as the germinal mathematical approach to modern "interest conflict" and game theory (Simon, 1959). Solving the generalized minimax theorem, von Neumann (1928) is also credited with conceptualizing the theory of games with more than two players (Luce & Raiffa, 1957). Unfortunately, game theory did not evolve considerably until 1944 when von Neumann and Morgenstern completed their groundbreaking book entitled *Theory of Games and Economic Behavior* (Kelley, 2003; Leonard, 1995). Written for mathematicians and economists, von Neumann and Morgenstern's germinal work on making decisions under conditions of certainty, risk, and uncertainty established the fundamental premises for modern utility theory (IFORS, 2006; Leonard, 1995).

Haywood (1954) first applied von Neumann's game theory to the art and science of military decision-making. In this germinal work, Haywood analyzed decisions from two World War II battles using two-person, zero sum game theory. According to Cantwell (2003), Haywood examined the various COAs to determine the value of the predicted outcomes. Contrary to the current doctrine of the time, Haywood found game theory techniques allowed the commander to analyze decisional risks based on the enemy's intentions rather than the enemy's capabilities alone. Although the idea of "mixed strategies" is more challenging with respect to applying game theory to military warfare, Haywood found U.S. doctrine to be overly conservative in this area.

Game theory has many applications for developing military decision-making strategies (Schultz, 1997; Cantwell, 2003). Similar to corporate decision processes, military leaders make multifaceted decisions under uncertainty that involve complex and ambiguous environments. Both manage constrained resources within highly interrelated systems. Even with automated decision-making tools that use state of the art information technologies, decision-makers seldom have complete situational awareness or a full understanding of the higher order effects and consequences of their decisions. Accordingly, private corporations have embraced game theory and statistical methods into their decision-making ideologies, analytical practices, and political economic models (Bueno de Mesquita, 2006; Cantwell, 2003). Based on the successes that businesses have experienced, Cantwell (2003) submitted military decision-making could also benefit from expanding the employment of game theory to strategic planning and risk modeling processes.

Bargaining theory. As described above, game theorists study strategic interactions between individual actors or groups of actors in cooperative and non-cooperative (competitive) environments. In this context, *bargaining* is considered a cooperative, nonzero sum game (Nash, 1950). In Nash's (1950) germinal work, a two-person bargaining situation entails two individuals with the opportunity to communicate and work together for achieving a mutual beneficial outcome. Therefore, in a true bargaining scenario, Nash assumed an individual could not take an action without the consent of the other if that action affects the other individual's wellbeing.

Building on the work of von Neumann and Morgenstern's (1944) game and utility theory, Nash (1950) developed bargaining theory on the classical problem of exchange. In general, an assumption of the bargaining problem is the actors are rational with equal bargaining skills. Furthermore, actors can compare and express their desire for preferred outcomes accurately with full knowledge of the preferences of each other. In addition, the concept of "anticipation" is important to understand and apply Nash's bargaining theory fully. In this context, Nash defined the anticipation of an individual as "a state of expectation, which may involve the certainty of some contingencies and various probabilities of other contingencies" (p. 156).

In 1953, Nash extended the original "bargaining problem" to a wider class of scenarios in which the concept of "threats" was introduced. Nash defined a threat in the following manner:

A threatens B by convincing B that if B does not act in compliance with A's demands, then A will follow a certain policy T. Supposing A and B to be rational

beings, it is essential for the success of the threat that *A* be *compelled* to carry out his threat *T* if *B* fails to comply. (p. 130)

Nash asserted that the *threat* is a necessary tool during a negotiation in which a negotiation is defined as a cooperative game. The word cooperative means that individuals can communicate, collaborate, and discuss the situation in order to agree on a rational and enforceable course of action or an agreement (Nash, 1953).

Nash (1950) suggested bargaining theory was applicable to economic situations of monopoly versus monopsony, trading between nation states, and labor union negotiations. Schelling (1956) extended Nash's work to include fundamental contributions to the development of stable conflict strategies (Ayson, 2000). Recognized as the one of the leading experts on modern strategic thought, Schelling's work on nuclear strategy in the late 1950s formed the underpinnings of the nation's nuclear deterrence policy that is still in effect today (Ayson, 2000).

Unlike Nash's (1950) bargaining theory in which cooperative communication between parties was assumed, Schelling (1960) developed strategic concepts based on tacit bargaining. Tacit bargaining, according to Schelling (1957), occurs when communication is incomplete or impossible. With tacit bargaining, Schelling (1956) proposed adversaries observe and interpret each other's behavior with the understanding their own actions are counter interpreted and used when making decisions based on expectations. The differences between Nash and Schelling's approaches to bargaining are founded on the premise that common interests and the desire to avoid a mutually undesirable outcome between the involved parties are achieved through the balance of deterrence (Ayson, 2000).

Reed, Clark, Nordstrom, and Hwang (2008) proposed that deterrence results from the balance of power. Reed et al. found a predication of bargaining theory is that the chance of hostilities occurring depends on the allocation of power and the *ex-ante* distribution of benefits. Normally, nation states achieve a negotiated balance externally using mutually favorable coalitions, agreements, and treaties or internally by exploiting or leveraging their own resources and capabilities (Reed et al., 2008). Consequently, Reed et al. determined that disparity between the division of power and benefits reduces the effectiveness of deterrence and increases the chances of war.

“OODA” loop theory. As one of the predominant models of military command and control, the Observe → Orient → Decide → Act (OODA) loop (see Figure 3) is a four stage, continuous, decision cycle in which the decision-maker interacts with the environment through a series of rational steps (Boyd, 1986; Brehmer, 2005; Schechtman, 1996). Developed as part of Boyd’s asymmetric fast transient theory of conflict, the goal of the decision-maker is to execute the OODA loop more quickly than an opponent can by reducing the *fog and friction* of information flow and processing (Clausewitz, 1873; Schechtman, 1996). Developed to explain U.S. fighter pilot success following the Korean War, Boyd (1976) introduced the OODA loop concepts after recognizing the need to “improve the capacity for independent action” (p. 1). Boyd’s (1986) OODA loop theory was the first warfare decision-making model that coupled physical space with cognitive space.

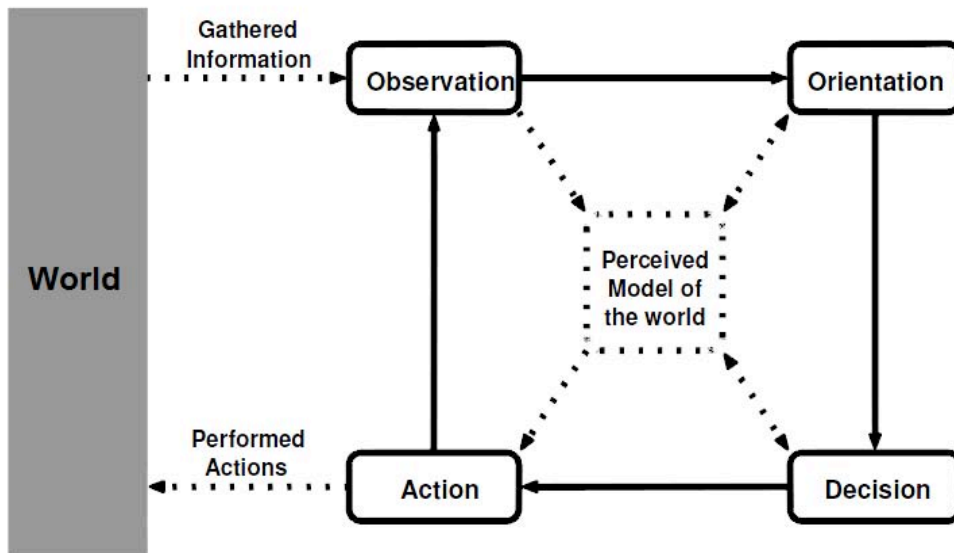


Figure 3. Boyd's (1986) original OODA loop model.

Reprinted with permission from "The Orientation Step of the OODA Loop and Information Warfare," by L. Brumley, C. Kopp, and K. Korb, 2006, Proceedings of the 7th Australian Information Warfare & Security Conference 2006, p. 19. Copyright 2006 by the Clayton School of Information Technology, Monash University, Australia.

By understanding how one develops conceptual patterns of meaning using destructive deduction and creative induction mental operations, Boyd (1976) demonstrated that conducting observations determines the state of a disordered system. Accordingly, the act of making observations reduces uncertainty and improves the decision-making process within complex environments (Boyd, 1976). In later work, Boyd (1996) expanded the OODA loop construct, illustrated in Figure 4, into a more generalized model intended to be applied to various forms of combat (Brehmer, 2005). Consequently, the OODA loop was transformed into a staged model with multiple feedback loops and an enhanced Orientation stage in which Boyd introduced mental

processes used by the decision-maker. The addition of feedback placed the modified OODA loop model into the cybernetic decision theory category (Brehmer, 2005).

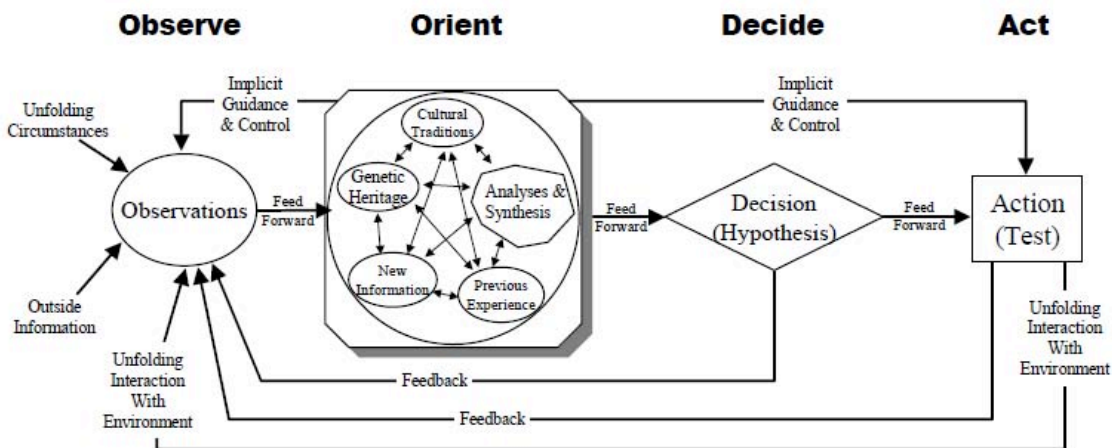


Figure 4. Boyd's (1996) modified OODA loop model.

Reprinted with permission from "The Essence of Winning and Losing," by J. R. Boyd, 1995, Department of Defense Briefing, p. 4. Copyright 2001 by the Defense and the National Interest.

In cyberspace, unlike physical domains, the speed of military operations approaches that of light (Mathers, 2007). With the ability to create nearly instantaneous effects on a global scale, cyberspace operations require decision-makers to execute the OODA loop stages with unprecedented speed, agility, and precision (Mathers, 2007). When making cyber warfare decisions, the limiting stage of the OODA loop is the Orientation step (Brumley, Kopp, & Korb, 2006; Studer, 2005). Recognizing the importance and challenges associated with decision-maker *orientation* is consistent with Boyd's (1986) general position on the subject.

Boyd (1986) stressed the importance of orientation by describing this phase as the "schwerpunkt" (i.e., focal point or center of gravity) of the OODA loop model (p. 16). During the Orientation stage, Brumley et al. (2006) found an individual's mental model of the world is a function of previous experience, cultural traditions, genetic heritage, as

well as cognitive analysis and synthesis. Because existing knowledge affects the interpretation of new information, Brumley et al. suggested that individuals who have contrasting representations of the world often envision dissimilar interpretations of the same event. Given these interpretive differences, the vast number of potential adversaries, and the sheer volume of data encountered in cyberspace, the time required to complete the Orientation step must be a fraction of that historically required for traditional warfare (Studer, 2005). When attempting to operate inside the adversary's OODA loop, the decision-maker must understand the Orientation step is often the limiting process.

Criticized for lacking widespread applicability and utility outside warfighting situations, Boyd never aimed to develop a general theory of decision-making (Brehmer, 2005). However, with the inclusion of feedback mechanisms and decision opportunities to the original construct, Boyd (1996) transformed the OODA loop into a cybernetic decision-making model. According to Brehmer (2005), the *cybernetic approach* is the predominant decision-making model on command and control. Builder et al. (1999) found that cybernetic models provide a highly useful basis and foundation for understanding *control* functions; however, these models are typically inadequate to depict the concept of *command* properly.

Builder et al. (1999) noted that adding components to cybernetic decision models based on cognitive science theory enhances the capability of these models to explain the decisional activities of individuals in command and control systems. Boyd's (1996) expanded Orientation step improves the OODA loop model in this fashion (Brumley et al., 2006). However, Builder et al. yielded that cognitive science does not model

command decision-making processes as accurately as control theory models automated control processes. Although the cultural and social aspects of decision-making historically are not incorporated in cybernetic approaches, Boyd's orientation process attempts to account for these human factors.

Builder et al. (1999) noted that cybernetic models are best suited for facilitating decisions over short time scales during the most intense stages of combat. Builder et al. found that cybernetic approaches dominate the decision-making models in environments with rapidly changing technology in which high-intensity, quick-reaction decisions are required. Therefore, according to Brehmer (2005), Brumley et al. (2006), and Mathers (2007), the OODA loop, when used as a cybernetic model, can support making effective cyber warfare decisions in the complex, dynamic, ubiquitous, and uncertain environment that characterizes the cyberspace domain.

Complexity Theory

Bennet and Bennet (2008) defined complexity as "the condition of a system, situation, or organization that is integrated with some degree of order, but has too many elements and relationships to understand in simple analytic or logical ways" (p. 1). Complexity theory has been applied successfully to chemical and biological systems, the social sciences, and organizational processes including cultural, political, and managerial dimensions (Murray, 1998, 2003). Complexity theory should apply to network centric warfare as well (Moffat, 2003). Within the current RMA, which started in the 20th century, Schneider (1997) suggested that complexity has emerged "as the defining characteristic of modern military organizations and operations" (p. 26). Furthermore, Schneider asserted that military information systems are *complex adaptive systems*

requiring leaders to use intuition and judgment to make warfighting decisions within dynamic and often unstable environments (Bennet & Bennet, 2008).

Complex phenomena, according to Hayek's (1964) germinal work, are characterized by abstract patterns resulting from the interactions between numerous variables. Complexity theory is used to describe the characteristics and dynamical behavior of complex adaptive systems using the foundational premises of systems theory, catastrophe theory, and chaos theory (Anderson, 1999; Glenn, 2002). According to Holland and Miller (1991), a complex adaptive system is *complex* when comprised of a network of interacting agents (processes or elements) that demonstrates a dynamic, collective behavior resulting from the individual activities of the coupled agents. Furthermore, the governing behavior of a complex adaptive system can be described adequately without a detailed understanding of the individual agents' subordinate activities (Holland & Miller, 1991). An agent in such a system is *adaptive* if the agent's actions can be characterized with a value that describes its performance or utility and the agent behaves in a manner to adapt to changing environmental conditions over time (Holland & Miller, 1991).

Systems theory. Following World War II, in conjunction with the development of computers, theorists began to model interactions instead of using simplifying assumptions that typically accompanied the reductionist methodology when describing intrinsically complex systems (Anderson, 1999). Attributed with the germinal work on general systems theory, Bertalanffy (1972) found that systems interact with their surroundings and modify or adapt their behavior based on the environment. Bertalanffy suggested that all real (non-theoretical) systems were open systems that required

interaction with other systems and the environment where matter and energy are exchanged. Using a living organism view of systems, Bertalanffy believed models, principles, and laws exist that describe the nature of a system's constituent elements and the force relationships between them. Using formulations such as wholeness and sum, differentiation, progressive mechanization, centralization, hierarchical order, competition, allometry, finality and equifinality, Bertalanffy determined dynamical systems theory could be applied to all open systems, living and constructed.

According to Blakesley (2005), systems are either dynamic or non-dynamic and linear or nonlinear. Dynamic systems have properties or characteristics that change over time. If a dynamic system is conservative, no net loss of matter or energy occurs. If a dynamic system is dissipative, net changes in matter or energy occur across the system boundaries. All real, dynamic systems are dissipative because energy is required to support the transfer of information or matter with the surrounding environment (Blakesley, 2005).

Systems also can be either linear or nonlinear (Blakesley, 2005). Linear systems have outputs proportional to inputs. With linear systems, internal processes can be modeled in a deterministic manner to predict input-output relationships accurately (Glenn, 2002). Nonlinear systems have outputs not necessarily proportional to inputs. Moreover, small changes to input values in nonlinear systems can dramatically affect the output values, causing the output to become erratic or stochastic (Blakesley, 2005; Glenn, 2002). Therefore, the performance of nonlinear systems is difficult to predict.

In general, systems are comprised of inputs, outputs, processes, boundaries, environment, and feedback (Glenn, 2002). Boundaries form the line of demarcation

between the system and the environment. The environment is anything external to the system that cannot be altered, affected, or influenced by the system. Feedback is the return of a portion of the system's output to the input. Feedback can be negative or positive. Negative feedback tends to dampen the system's output in a manner to return the system back to its original or equilibrium state (Glenn, 2005). In contrast, positive feedback causes the system to move further and further from its original state by reinforcing the input to output ratio (Blakesley, 2002). Negative feedback helps restore system stability. Positive feedback causes system amplification and eventual instability (Blakesley, 2002).

Cybernetics. Wiener (1948) founded cybernetics to describe the communication and control theory necessary to improve anti-aircraft guns and missile system performance during World War II. Defined by Wiener as the art of *steermanship*, cybernetics is the scientific treatment of coordinated regulation and control using feedback loops (Ashby, 1956). Ashby (1956) recognized that cybernetics provided a set of effective methods and techniques for examining, managing, and controlling systems intrinsically and exceedingly complex.

Forming two of the four fundamental pillars of complexity theory, cybernetics and general systems theory are used to explain how internal system elements relate and communicate in order to function holistically (Glenn, 2002). General systems theory is improved using cybernetics to describe how a complex system behaves and interacts with its environment in response to external stimuli using the concept of feedback and the principles behind control (Glenn, 2002). Specifically, cybernetics is used determine how

the state of a system changes between incremental time units T and $T+\Delta T$, which is essential to the determination of system stability (Ashby, 1956).

Cybernetics forms the basis of cybernetic decision-making theory previously described. An example of cybernetics in operation, according to Glenn (2002), occurs in conjunction with the “CNN effect” (p. 23). The CNN effect occurs when decision-makers feel forced or compelled to react to sensational news media pressure in order to make foreign policy decisions before they normally would absent the media coverage (Belknap, 2001; Livingston, 1997). According to Livingston (1997), the CNN effect is a “policy agenda-setting agent; an impediment to the achievement of desired policy goals, and an accelerant to policy decision-making” (p. 4). From cybernetics theory, Glenn asserted the CNN effect creates a new model of the situation caused by the observation of the news media coverage, which quickly couples the decision-maker to the sensationalized event. This new and dynamic relationship with rapidly changing boundary conditions causes decision-makers to interact (and frequently overreact) in order to keep the overall system stable using the media coverage as feedback for controlling their efforts (Glenn, 2002).

Chaos theory. Chaos theory is the study of nonlinear, dynamic systems (Blakesley, 2005). First discovered while attempting to solve the “three-body problem” (i.e., the orbital equations of motion for a system of three independent bodies), Poincaré (1890) uncovered two important findings (Blakesley, 2005). First, Poincaré found a system of three bodies bounded by gravity could not be expressed with a closed-form, analytical solution. Second, Poincaré noticed that a small variation in the initial input values to the system (e.g., position, velocity, mass) resulted in large discrepancies in the

predicted outcome of the final state (Blakesley, 2005). Therefore, Poincaré is credited with mathematically describing the first chaotic, deterministic system.

The study of chaotic systems faded until Lorenz (1963) found similar results to Poincaré while studying weather systems and air currents. For weather systems with bounded solutions, Lorenz determined that non-periodic solutions are usually unstable with regard to small perturbations. Therefore, introducing slight variations to a system's initial state can result in the system evolving into considerably different final states (Lorenz, 1963). These findings led Lorenz (1972) to postulate what became known as the "butterfly effect." Specifically, Lorenz extended the work on weather systems to suggest that a butterfly flapping its wings in Brazil could cause a tornado in Texas. This ludicrous hypothesis was Lorenz's attempt to illustrate the instability that chaotic systems exhibit through a sensitive cause and effect relationship.

Although chaotic systems are dynamic, non-periodic, and appear to behave randomly, they are deterministic (Thiéart & Forgues, 1995). Even though Poincaré (1890) and Lorenz (1963) found forecasting exact values of future chaotic system states challenging, Anderson (1999) reported these systems normally achieve equilibrium around a confined region of the space, called a *strange attractor*, where the system permanently resides. Blakesley (2005) noted that analyzing the "attractors" associated with a chaotic system helps determine the period of stability. Understanding the dynamics of chaotic systems highlights the need for agile and flexible military decision-making processes within complex environments (Blakesley, 2005).

According to Qvortrup (2006), chaos theory has emerged as a vital theory within the fields of digital media networks and communication systems. Applying chaos theory

to computer network models can improve the understanding of undesirable second and third order effects, which can result from a cyber attack (Atkinson & Moffat, 2005; Butler et al., 2005). A byproduct of the ever-growing scale, complexity, and pace of operations, Atkinson and Moffat (2005) noted that battlespace chaos appreciably increases decision-making intricacy and uncertainty. To improve a leader's confidence when making cyber warfare decisions in which unintended or unanticipated collateral effects could cause unacceptable risk, Butler et al. (2005) recommended integrating chaos and complexity into the analytical structures and systematic frameworks for making decisions. Consequently, Smith (2006) suggested an effects-based approach to decision-making is appropriate in highly connected, networked environments using complex adaptive systems to model the desired effects and subsequent end states.

Catastrophe theory. Catastrophe theory, first described by Thom (1972) in the germinal work on the theory of models, is essential for understanding complex, deterministic systems (Anderson, 1999; Murray, 2003). Catastrophe theory, a branch of bifurcation theory, predicts how small changes or perturbations in physical parameters can cause a system to change abruptly from one equilibrium state to another (Anderson, 1999; Thom, 1972). According to Lanza (2000), catastrophe theory is a “general theory for describing and predicting discontinuous changes in events” (p. 59). Derived from topology (i.e., the study of surfaces with many dimensions), catastrophe theory is used with this branch of mathematics to describe the underlying natural forces using smooth surfaces in equilibrium (Knight, Tulloch, & Knight, 2004). Catastrophes occur when discontinuities emerge along an equilibrium surface (Lanza, 2000).

Catastrophe theory has many applications such as modeling human emotional responses to changing circumstances, stock market surges and crashes, societal behavior, computer network performance, and decision-making processes (Lanza, 2000; Nelson, 1987). Building on Kahneman and Tversky's (1979) work on decision framing, Syvvyantek, Deshon, and Siler (1991) used catastrophe theory to describe the unexpected and abrupt shifts in preference resulting from visual illusions and perceptual synthesis. The decision framing phenomenon occurs when a decision is altered following the presentation of objective information to the decision-maker in which the expected success probabilities of the different alternatives are known (Kahneman & Tversky, 1979).

In the physical, non-theoretical world, catastrophes are extremely difficult to predict. According to Taleb (2007), catastrophes can be illustrated by a "black swan" metaphor. In this context, Taleb described black swans as unpredictable events with substantial consequences where, after the fact, explanations are concocted to provide the impression that the event was not random but predictable using existing theory and processes. Examples of black swans are the rise of Hitler, the 9/11 attacks, the rise and fall of the Soviet bloc, and the globalization of the Internet.

Among the countless *black swans* that could occur without notice, Goure (2008) suggested a "Cyber Pearl Harbor" event (i.e., a large-scale cyber attack against U.S. critical infrastructures) is a possibility within today's strategically uncertain environment. Because black swans are inevitable, Goure recommended the military employ capabilities-based (versus threat-based) planning processes because they are versatile, adaptive, and capable of providing decision-makers with rapid response options designed

to combat catastrophic events worldwide. Without a thorough understanding of the factors, risks, and uncertainties that characterize a cyber event, Butler et al. (2005) emphasized that decision-makers will not have adequate confidence to make quality warfare decisions. Bennet and Bennet (2008) found decision-making under highly uncertain and complex circumstances requires a conceptual appreciation of the butterfly effect, tipping points, feedback loops, and power laws that govern catastrophic events.

Deterrence Theory

Deterrence theory is a critical component of the overall theoretical framework for this research study (see Figure 2). The concept of deterrence is inherently associated with the measures taken to encourage restraint, deny benefits, or impose costs to an adversary (Cartwright et al., 2006; Sharp, 2008; Taipale, 2009). The effectiveness of deterrence has traditionally been directly related to a nation's ability and resolve to respond creditably and decisively with force (Kunsman & Lawson, 2001). However, in cyberspace, the complexity of the environment coupled with the substantial number of actors with substantive attack capabilities makes deterring malicious behavior a more daunting task (Jervis, 1997; Kugler, 2009; Taipale, 2009). In this section, traditional and cyber deterrence theories are presented in order to highlight the challenges that must be overcome when developing a legitimate deterrence policy for making response decisions to cyber attacks.

Traditional deterrence theory. In 1959, Brodie defined deterrence as “the prevention from action by fear of the consequences” (p. 34). Using this definition, historian Howard (1994-95) postulated a “strategic paradigm based on deterrence, compellence, and reassurance . . . where military power can deter other states from doing

something, compel them to do something, or reassure them of a general sense of security” (p. 165). In 1997, Keyes et al. published one of the first noteworthy reports that highlighted the differences between classical deterrence and cyber deterrence. Specifically, Keyes et al. realized, in cyberspace, the United States cannot rely on any advance warning time to dissuade a potential adversary or take preemptive action to prevent a cyber attack. These challenges are exacerbated because the United States currently lacks the capabilities and policies to serve as a credible deterrent to potential adversaries (Keyes et al., 1997; Taipale, 2009).

In this germinal work, Keyes et al. (1997) proposed a three-step process toward building an effective cyber deterrence strategy. First, the president should declare a policy and build international consensus. Second, U.S. government agencies and departments should harden potential targets and impede/deny access to them. Last, the U.S. government should broadly share information, thoroughly conduct analysis of cyber attacks, and issue warning notices concerning discovered threats and vulnerabilities (Keyes et al., 1997).

Building on Keyes’ et al. (1997) concepts, Khalilzad (1999) proposed three basic strategies for defending against cyber warfare: protection, deterrence, and prevention. In Khalilzad’s construct, protection reduces vulnerabilities by increasing resiliency through hardening potential targets, reducing the resultant damage, and improving the capability to recover expeditiously. Deterrence, according to Khalilzad, reduces the motivation for malicious actors to conduct network warfare based on credible retaliatory capabilities. Finally, prevention reduces the capacity and hinders the capability for adversaries to obtain and effectively employ cyber weapons and techniques (Khalilzad, 1999).

The success of Cold War deterrence primarily is the result of decision-making conducted by a small group of rational actors (i.e., nation states) empowered by the confidence instilled through credible technological advantage (i.e., nuclear devices) and the reasonable certainty of attributing the weapon release event (Kunsman & Lawson, 2001). Furthermore, DoD leaders have considerable experience making warfare decisions that leverages an extensive body of knowledge centered on strategic deterrence theory and policy relating to WMD (Neary, Preisinger, Ludka, & Sutter, 2001). Because many DoD leaders consider a large-scale cyber attack equivalent to using WMD, the question remains why so much uncertainty exists when considering using force in response to such an attack.

By examining the assumptions that leaders consider when making decisions to use force against the threat of traditional WMD, marked differences emerge when contrasted to cyber attacks. According to Cartwright et al. (2006), the assumptions that contribute to the “goal of deterring attacks . . . through decisive influence on the adversary’s decision calculus to attack are . . . the result of an awareness of an adversary’s attack capabilities” (p. 11). Cartwright et al. noted that only actions that result from deliberate and intentional decisions (i.e., not from automatic responses or unintended/accidental events) can be deterred. Moreover, deterrence strategies must identify and assess the adversary’s values and perceptions relevant to their decision-making calculus and worldview (Cartwright et al., 2006). Finally, an assumption of classical deterrence is the existence of actual irrational actors (i.e., those who make decisions randomly without regard to anticipated outcomes) is extremely rare (Cartwright et al., 2006).

In *The National Defense Strategy*, Secretary of Defense Rumsfeld (2005)

highlighted the need for a comprehensive and effective deterrence policy designed to dissuade attacks from adversaries to ensure the security of the United States. This pre-emptive policy should deter attacks including those in cyberspace that affect our way of life (Rumsfeld, 2005). In order for a deterrence policy to be effective, leaders should be able to identify the adversary; the adversary believes the United States has the means and resolve to inflict costs or deny benefits; and the adversary wishes to avoid these consequences (Brodie, 1959; Cartwright et al., 2006; Schelling, 1960).

Cyber deterrence theory. Barnett (1998) first proposed applying the concept of deterrence to information warfare with the articulation of a U.S. cyber deterrence policy. However, some argue, according to Kugler (2009), that modern-era adversaries cannot be deterred because they are not rational and thus, not “influenced by the same cautionary mechanisms that motivate normally sensible actors” (p. 36). However, Kugler argued that “rationality” is a relative term. While some of today’s actors may not be rational by traditional standards, Kugler concluded they are not entirely irrational. Even today’s violent extremists are governed by explicit motives, goals, and awareness of costs and risks. Kugler found these principles hold true for nation states, and apply, to varying degrees, to non-state actors. Even terrorist groups are “motivated not just by ideology and hatred, but also by strategic goals and self-preservation” (Kugler, 2009, p. 36).

Before a cyber deterrence policy can be effective, Khalilzad (1999) asserted that a cyber deterrence theory should address the fundamental differences between conventional, nuclear, and cyber warfare. To this point, Khalilzad considered several characteristics are required to make deterrence successful within the information-warfare

context. First, Khalilzad recognized that a clear, declaratory policy must specify the expected level of behavior along with the consequences an aggressor can anticipate following an attack. Next, for the declaratory policy in cyberspace to be executable, the United States must have the ability to identify an attack and the attacker. Finally, for deterrence to be enduring, the United States must establish credibility by demonstrating the willingness to respond to attacks using all elements of national power.

Kugler (2009) developed a cyber deterrence theory by extending the principles associated with Brodie's (1946, 1959) and Schelling's (1966) classical strategic deterrence theories while accounting for the technical, social, and cognitive distinctions inherent to cyberspace, which were highlighted by Keyes et al. (1997) and Khalilzad (1999). Kugler asserted a "one-size-fits-all approach to [cyber] deterrence will not work because of the multiplicity and diversity of potential adversaries and cyber attacks" (p. 15). Therefore, a cyber deterrence theory should be "tailored" to treat each category of potential adversary, type of attack, and type of response on its own merits (Kugler, 2009).

Kugler (2009) described a general model for accomplishing tailored cyber deterrence by employing instruments of national power to influence a potential adversary's physical, psychological, and motivational centers of gravity using an ends, ways, and means construct. *Ends* are objectives, expressed as verbs (e.g., deter cyber warfare, promote appropriate Internet behavior), designed to achieve the desired end state (Bartholomees, 2008). *Ways* are the strategic concepts and COAs that determine how the ends are attained using properly distributed resources (Bartholomees, 2008). *Means* are the tangible or intangible assets (e.g., forces, capabilities, and equipment) that delineate the specific resources required to achieve the objectives (Bartholomees, 2008).

According to Kugler (2009), cyber deterrence requires a coordinated approach employing all elements of national power with defensive response options that contain more than purely cyber-related alternatives. Because the span of hostile actors that must be deterred ranges from nation state sponsored activities to asymmetric terrorism to criminally based hacktivism, a robust deterrence theory should be generalizable to a broad spectrum of cyber warfare responses. Therefore, Kugler warned that leaders should evaluate use of force thresholds carefully because cyber attacks occur in various degrees. Consequently, a response to a cyber attack should consider the principles of necessity, proportionality, unnecessary collateral damage, injury to civilians, and anticipatory self-defense (Barnett, 1998; Sharp, 1999a).

A cyber deterrence strategy should contribute to other key defense activities and goals, including assurance of allies and dissuasion (Kugler, 2009). According to Kugler (2009), dissuading adversaries is crucially important and not an easy task. Whereas deterrence is the “logic of direct military coercion applied against a hostile, well-armed enemy,” Kugler (2002) defined dissuasion as an “effort by the United States to convince a country or coalition to refrain from courses of action that would menace our interests and goals” (p. 1). Kugler believed leaders should use dissuasion as a complement or an enabler to a cyber deterrence policy. Because absolute deterrence against malicious activity in cyberspace is highly unlikely, cyber dissuasion is vital and requires the U.S. government invest heavily in technical capabilities while building deconfliction processes necessary to employ these capabilities effectively across the interagency (Kugler, 2009).

According to Chesser (2007), “Decision makers, policy makers, and commanders at all levels need to understand deterrence theory applicable to the 21st century security

environment” (p. 1). Specifically, Chesser advised that leaders require a deterrence typology in order to grasp the complex methods to deter non-nation-state actors while concurrently bolstering the means to deter and compel nation states. Chesser’s theoretical deterrence model relies on a deterrence analysis and planning support environment founded on an effects-based paradigm that requires a thorough understanding of the tailored deterrent effect desired for the specific situation. In this model, deterrence is accomplished through a five-step process. First, the planner specifies the deterrence objectives and the appropriate strategic context (Chesser, 2007). At this stage, actors are identified by their decision-making capabilities and contextual properties using a guidance typology (Chesser, 2007).

During the next step, the planner assesses the decision calculus of each actor by defining the relevant interests and agendas. In the third step, leaders identify desired deterrence effects on the actors’ decision calculus and influence levers (Chesser, 2007). Operational analysts test the influence levers using models, subject matter experts, and other sources during the fourth step. Finally, decision-makers conduct a “DIMEFIL” (diplomatic, information, military, economic, financial, intelligence, law enforcement) evaluation to determine which element (or combination of elements) of national power would best achieve the desired deterrence effects (Chesser, 2007).

Chesser’s (2007) deterrence model is built on generalized classical decision theory, which is commonly comprised of utility and probability theories, to include performance measures and uncertainty theories (Eberbach, 2005). Because deterrence theory ultimately is used during the process of making extremely vital decisions, Edwards (1954) behavioral decision-making theory is essential for framing the levers of

influence and for determining the achievability and effectiveness of deterrence objectives (Bullock, 2006). Chesser used von Neumann and Morgenstern's (1944) game theory as well as Suh's (1999, 2005) complexity theory to form the foundational premises of the decision-making process associated with multiple outcomes within complex systems. Furthermore, Chesser leveraged Schelling's (1960, 1966) bargaining theory and strategic deterrence theory when developing the decision processes to determine the thresholds in which military action is necessary to prevent escalation or intensification.

Schmitt Decision Analysis

Perhaps the most developed and scrutinized treatment regarding cyber warfare decision-making should be credited to Schmitt's (1999) germinal work on determining when a CNA constitutes the use of force under international law (D. Denning, 2007). Known as the "Schmitt Analysis," Schmitt proposed a normative framework based on evaluating the consequences associated with a cyber attack in comparison to a kinetic attack using the United Nations (UN) Charter as the legal basis. Schmitt proposed seven criteria that decision-makers can use when evaluating if an attack warrants the use of force. Centered on the UN Charter's Article 2[4] (use of force exclusion), Chapter VII (peace and security restoration), and Article 51 (inherent right to self-defense), the Schmitt Analysis facilitates understanding the spectrum of response options that decision-makers should consider following a hostile act (D. Denning, 2007; Schmitt, 1999).

Prior to Schmitt's (1999) analytical treatment, two schools of thought prevailed when determining if an attack warranted the use of force under international law (Michael et al., 2003). The first, known as the "common sense" approach, focuses primarily on the amount of damage resulting from an attack, independent of the method

of attack. In this case, the kinetic legal regime is directly applicable to cyberspace. Although this approach has the benefit of simplicity, clarity, and logic, Michael et al. (2003) warned this method is problematic with regard to the existing international law paradigm and the UN Charter structure. More popular in academic environments, the second approach applies the UN Charter's logic using a literal interpretation in which any action except an armed attack is allowable. With this understanding, the amount of force matters less than the type of force. Whereas this approach allows response action thresholds or "red lines" to be easily determined, Michael et al. cautioned this method fails to account for the destructive effects of modern cyber attack capabilities.

These two schools of thought divided most academic and legal discussions regarding decisions to use of force following an attack until Schmitt (1999) proposed a methodology for normalizing kinetic and non-kinetic attacks. According to Schmitt (1998), "As the nature of a hostile act becomes less determinative of its consequences, current notions of 'lawful' coercive behavior by states, and the appropriate responses thereto, are likely to evolve accordingly." (p. 1056). To capture the essential elements and quantify the evolution of response actions decision-makers face as modern warfare becomes more irregular and asymmetric, Schmitt (1999) examined the UN Charter in order to understand how the framers characterized each type of coercion. From this evaluation, Schmitt suggested a quantitative scale (e.g., 1 to 10) be applied to seven descriptive factors that translated the qualitative nature of the UN Charter into an analytical framework for evaluating the use of force following an attack.

The seven criteria Schmitt (1999) considered during the normative framework development are severity, immediacy, directness, invasiveness, measurability,

presumptive legitimacy, and responsibility. Severity is the degree that people are killed, wounded, or the scope of property damage. Immediacy is the time after an attack before the consequences take effect. Directness is the correlation between an attack and its effects. Invasiveness is the degree an attack required a nation's sovereign borders to be crossed. Measurability is the extent to which the efficacy of an attack can be measured. Presumptive legitimacy is the extent to which the international community considers an attack legitimate. Responsibility is the degree that an attack can be linked to a particular nation state or other malicious actors.

To demonstrate how the Schmitt Analysis criteria apply to a cyber attack, D. Denning (2007) proposed the following example:

Consider an intrusion into an air traffic control system that causes two large planes to enter the same airspace and collide, leading to the deaths of 500 persons onboard the two aircraft. In terms of severity, the cyber attack clearly ranks high. Immediacy is also high, although the delay between the intrusion and the crash may be somewhat longer than between something like a missile strike and the planes crashing. With respect to directness, let us assume the reason for the crash is clear from information in the air traffic control computers and the black boxes onboard the planes, so directness ranks high. Invasiveness, however, is moderate, requiring only an electronic invasion rather than a physical one. Measurability, on the other hand, is high: 500 people dead and two planes destroyed.

Presumptive legitimacy is also high in that the act would be regarded as illegitimate, akin to a missile attack (the high end of the spectrum corresponds to high illegitimacy). Responsibility comes out moderate to high. In principle, the

perpetrator could be anyone, but the level of skill and knowledge required to carry out this attack would rule out most hackers, suggesting state sponsorship. (p. 6)

In summary, five criteria (severity, immediacy, directness, presumptive legitimacy, and measurability) scored high, while the remaining two criteria (invasiveness and responsibility) scored moderate. Therefore, D. Denning suggested that the cyber attack in this example would resemble the use of force more than other legitimate forms of coercion.

After conducting an evaluation of how the Schmitt Analysis criteria apply to cyber warfare, Rowe (2007) determined cyber attacks rank high on the immediacy and invasiveness scale; however, depending on the methods used, their effects can vary greatly with regard to severity, directness, and measurability. Rowe found no presumption of legitimacy for cyber attacks while noting that responsibility is extremely difficult to assign in cyberspace. Rowe's observations capture the complexity and uncertainty of cyber attacks by emphasizing the attribution challenges faced by military officers when making decisions regarding the use of force. Although Rowe found the Schmitt Analysis to be a useful framing construct to the cyber attack problem, applying the seven criteria, including the spectrum of consequences and the necessary supporting evidence, would be difficult to accomplish in practice.

Legal Aspects of Cyber Warfare

The legal aspects of cyber warfare are perhaps the most contentious and complex issues that are faced when determining the response to a cyber attack (Carr, 2010; Owens et al., 2009; Schmitt, 2006; Wingfield & Michael, 2004). When considering the legality of cyber attacks, the effects of the attack must be considered more important than the

modality (Owens et al., 2009; Robertson, 2002). Adding to the legal complexity, clearly defined parallels between traditional and cyber response options that are supported by historical precedence and international agreement have not been established (Schmitt, 2002, 2006). In this section, the legal aspects of cyber warfare are explored through (a) international law, (b) the North Atlantic Treaty, and (c) the rules of engagement and the inherent right of self-defense.

International law. When the legal community first considered the concept of military activities in cyberspace, Sharp (1999a) noted the initial consensus among many U.S. government attorneys was that this area of warfare was so nascent that *no law* applied. However, after years of legal research, contemplation, and debate, most principles of international law were generally found applicable to the use of force in cyberspace (Schmitt, 1998, 1999; Sharp, 1999a). For the purposes of analyzing what warrants the use of force, three distinct categories of international law are relevant for exploration. These three legal regimes are summarized as the law of peace (*jus in pace*), the law of conflict management (*jus ad bellum*), and the law of war (*jus in bello*), otherwise known as the law of armed conflict (Sharp, 1999a; Wingfield & Michael, 2004). Depending on the phase of a particular conflict, Wingfield and Michael (2004) asserted, “Decision-makers must have sound, fact-based legal advice that is connected to clearly articulated principles of law” (pp. 9-10) prior to making use of force decisions.

The peacetime regime of international law (*jus in pace*) governs the conduct of nation states during times of peace using treaties and agreements (Sharp, 1999a). The law of conflict management (*jus ad bellum*) is a part of the peacetime regime of international law that defines and governs the use of force during peace. Before armed

conflict occurs, the law of conflict management obligates nation states to terminate hostilities consistent with their self-defense (Sharp, 1999a). The law of armed conflict (*jus in bello*) governs the conduct of hostile actions. This body of law, according to Sharp (1999a), purposely provides the authorization for a wide range of force during armed conflict that would typically be unlawful during peacetime. In Appendix D, Sharp (1999a) illustrated the spectrum of nation state activities against the legal thresholds and range of responses allowed under international law.

When considering the response to a cyber attack, Wingfield and Michael (2004) noted that the decision-making must consider where along the spectrum of international activities (i.e., “line of belligerency”) the attack occurred. As a matter of the international law, the use of force by a nation state initiates an armed conflict (Wingfield & Michael, 2004). When this occurs, a nation state is legally authorized “to use all necessary and proportional force not otherwise prohibited by the law of armed conflict that is required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources” (Wingfield & Michael, 2004, p. 10). As historically evidenced by traditional (i.e., kinetic) armed conflicts, this logic and legal standard has proven to be relatively straightforward in application. Unfortunately, the same cannot be said about cyber attacks (Schmitt, 1999; Sharp, 1999a; Wingfield & Michael, 2004).

Consequently, Wingfield and Michael (2004) proposed two fundamental questions that military leaders must address when responding to a cyber attack:

1. Which interstate activities in cyberspace constitute a threat or use of force under international law; and

2. When such a threat or use of force does constitute an armed attack under international law, how does the law of armed conflict apply to the lawful exercise of the inherent right of self-defense in cyberspace? (p. 10)

These questions are essential to the law of information conflict (LOIC). According to Wingfield and Michael (2004), the LOIC is the combination of the peacetime regime, the law of conflict management, and the law of armed conflict that governs nation state activities in cyberspace. When determining the appropriate LOIC response to a cyber attack, Peng, Wingfield, et al. (2006) proposed the decision tree shown in Figure 5. In Figure 5, Presidential Executive Order 12333 is the policy directive for national intelligence activities. The term “Resources” implies that additional information is required prior to making the legal response action decision.

Traditionally, legal scholars approached answering the first question above using a quantitative approach in which the emphasis was primarily on the end state of the attack versus the ways or means of how the attack was conducted (Wingfield & Michael, 2004). Specifically, a cyber attack should be indistinguishable from a kinetic attack if similar physical damage occurred. In this case, international law is generalizable to the LOIC and can be applied seamlessly when determining the appropriate response action. Unfortunately, the UN Charter takes a qualitative approach regarding the international laws of conflict by emphasizing the non-military methods of coercion such as diplomatic and economic versus the use of force. The Schmitt Analysis helps decision-makers with this intellectual and legal dichotomy by providing a framework for distinguishing between how military operations differ qualitatively from nonmilitary activities.

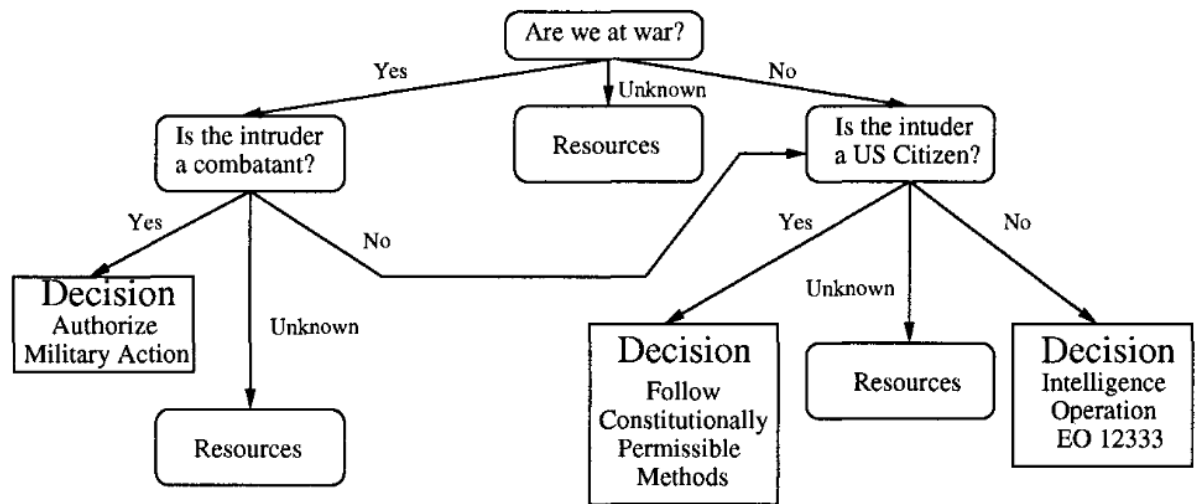


Figure 5. Decision tree for determining legal response actions.

Reprinted with permission from “Making Legal Decisions about Legal Responses to Cyber Attacks,” by L. Peng, T. Wingfield, D. Wijesekera, E. Frye, R. Jackson, and J. Michael, 2006, *Advances in Digital Forensics*, p. 290, Copyright 2006 by the Boston, MA: SpringerLink.

North Atlantic Treaty applicability. Under standard international law, armed conflict is perceived as “[any] difference arising between two States and leading to the intervention of armed forces . . . even if one of the Parties denies the existence of a state of war” (Tikk et al., 2008, p. 11). International humanitarian legal principles apply when cyber attacks are attributable to a particular State; the attacks are more than random, unrelated incidents; and the attacks are intended to cause injuries, casualties, or considerable damage (Tikk et al., 2008). When these criteria are met, the North Atlantic Treaty for members of NATO also applies.

Tikk et al. (2008) stressed that members of NATO must consider whether Articles 4 and 5 of the North Atlantic Treaty apply following the use of force or an armed attack prior to invoking the response actions provided by the treaty. In Article 4, “the Parties will consult together whenever, in the opinion of any of them, the territorial integrity,

political independence, or security of any of the Parties is threatened” (North Atlantic Treaty, 1949, Article 4). For purposes of responding to an attack, the applicable portions of Article 5 apply. Specifically, the “Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all” (North Atlantic Treaty, 1949, Article 5). Following an armed attack, members of NATO can use the means deemed necessary, including armed force, to assist the attacked Party by exercising “the right of individual or collective self-defense” in accordance with Article 51 of the UN Charter, (North Atlantic Treaty, 1949, Article 5).

Tikk et al. (2008) designed the following threshold test for determining the applicability of Article 5 (i.e., Collective Defense Article) in order to facilitate the decision-making process following a cyber attack:

1. Is the applicant a member of NATO?
2. Is the Nation under cyber attack?
3. Does the cyber attack constitute an armed attack?
 - a. Is there participation of armed forces; or
 - b. Is the attack attributable to a State?
 - (1) Is it directed by the State; or
 - (2) Is it supported by the State; or
 - (3) Is it tolerated by the State; or
 - (4) Is the State inactive?
4. Does the cyber attack constitute an attack in the meaning of international humanitarian law (i.e., an act of violence)?
 - a. Does the attack result in damage/destruction; or

b. Does the attack result in injury/death? (p. 21)

By answering these questions affirmatively, Tikk et al. (2008) suggested that Article 5 most likely applies. Therefore, the nation state under cyber attack can request the assistance of other NATO members and respond with proportional force, treating the cyber attack as an armed attack.

Rules of engagement and inherent right of self-defense. Rules of engagement are the “implementation guidance on the application of force for mission accomplishment and the exercise of the inherent right and obligation of self-defense” (Shelton, 2000, p. A-1). Accordingly, a “commander has the authority and obligation to use all necessary means available and to take all appropriate actions to defend that commander’s unit and other U.S. forces in the vicinity from a hostile act or demonstration of hostile intent” (Shelton, 2000, p. A-3). The inherent right of self-defense empowered through the formal rules of engagement applies in all warfighting domains, including cyberspace (Doyle, 2002). Unfortunately, the thresholds for determining a hostile act is extremely challenging in cyberspace. Furthermore, the differentiation between cyber crime and cyber attacks can be so subtle that determining hostile intent is even more difficult.

Cyber attacks are uniquely complicated because they can be directed toward either resident data or physical computer network systems. Therefore, the decision-maker must evaluate the effects of the attack and not necessarily the means or methods of the attack when determining if a hostile act occurred (Doyle, 2002). Because experiencing and evaluating the consequences of a cyber attack are essential for deciding on the proper response action, determining if an adversary is demonstrating hostile intent is nearly impossible due to the nature and speed of malicious cyberspace activities. More

specifically, cyber attacks can occur at speeds near that of light with little notice causing a large range of consequences.

According to Doyle (2002), cyber attacks can span a large range of severity. Doyle found cyber attacks are scalable and capable of rising to the level of an armed attack causing destruction of property, suffering, severe injury, and death. However, in most cases, cyber attacks are normally just annoying or intrusively disruptive with no imminent threat to life. In both cases, commanders rely on the rules of engagement to make decisions regarding the appropriate defensive response action, if any, to take. Doyle asserted, “The standing rules of engagement bridge the transition between *jus ad bellum* and *jus in bello* by implementing the inherent right of self-defense and providing guidance for the application of force to accomplish the mission” (pp. 150-151).

When determining how to respond to an attack or a use of force, the decision-maker must characterize the legal regime of the malicious activity as law enforcement, intelligence collection, or military operation (Peng, Wingfield, et al., 2006). Because an attack can cross many jurisdictional boundaries, Peng, Wingfield, et al. (2006) warned that merely terminating the connection or aggressively responding back in kind (i.e., using the same attack method as the counterattack) can have unintended consequences and in the worse case, be illegal. Therefore, when exercising the inherent right of self-defense in cyberspace, the commander must still adhere to the customary rules of war: distinction, necessity, proportionality, and chivalry (Peng, Wingfield, et al., 2006).

In this context, the principle of *distinction* (or discrimination) necessitates that commanders differentiate between combatants and noncombatants as well as between military and civilian objectives prior to authorizing the use of force (Wingfield &

Michael, 2004). The principle of *necessity* allows the commander to use the force required (or necessary) to accomplish the tasked mission while not applying excessive force or causing unnecessary suffering (Wingfield & Michael, 2004). The principle of *proportionality* requires the commander to respond to a hostile act or demonstrated hostile intent with reasonable, proportional force commensurate with the perceived or established threat while minimizing collateral damage to noncombatants (Kelsey, 2008). Lastly, the principle of *chivalry* allows ruses of war, but prohibits unlawfully deceiving (i.e., perfidy) an opponent by using entitled protections of law (e.g., vehicle displaying a Red Cross symbol; Wingfield & Michael, 2004). The rules of war apply in cyberspace and form a necessary (not sufficient) set of criteria for deciding on the appropriate defensive response action following a hostile act or hostile intent.

Examples of Cyber Attacks

Large-scale cyber attacks are a real and growing threat to national security (Bruno, 2008; Crovitz, 2008). Compounding the problem are the attribution challenges resulting from cyber attacks conducted by nation state sanctioned proxies from literally anywhere in the world (Korns & Kastenber, 2008; Report to Congress, 2007; Taipale, 2009). Therefore, determining the appropriate response based on domestic law, international treaties, sovereignty considerations, and the law of armed conflict is extremely difficult (Crovitz, 2008; Tikk et al., 2008). This section provides examples in which cyber attacks were conducted against (a) Estonia, (b) Georgia, and (c) the Pentagon.

Estonia. In April 2007, a cyber attack was conducted against many Estonian government, political, financial, corporate, and media websites (Kampmark, 2007). The

attack commenced after Estonian officials relocated a bronze Soviet-era war memorial recognizing an unknown Russian soldier who died fighting Nazi Germany (Vamosi, 2007). Although moving the statue seemed innocuous, the action infuriated the Russians living in Tallinn, the capital of Estonia. According to Kampmark (2007), the statue had become a central landmark for anti-government activists, “a talismanic presence for Russian protesters” (p. 288). The move provoked rioting by ethnic Russians in front of the Estonian Embassy in Moscow (Vamosi, 2007).

Following the rioting, Estonia experienced a crippling distributed denial of service attack of unprecedented scale for more than three weeks (Traynor, 2007). Kampmark (2007) reported the websites of the Justice and Foreign ministries were inundated with excessive requests using botnets from Russian computers. The cyber attacks took other forms as well. Chat forums and blogs were used to increase the scope of the event by posting instructions on how to use malicious cyber tools to overwhelm the Estonian government websites with bogus requests. Websites were defaced with Russian propaganda using electronic graffiti as a type of cyber scrawl. The cyber attacks on Estonia, according to Landler and Markoff (2007), marked a watershed event in terms of exposing the vulnerability of Estonian’s modern and technologically enabled society.

Estonian Defense Minister Aaviksoo asserted the cyber attacks against Estonia were equivalent to armed attacks under Article 51 of the UN Charter. Defense Minister Aaviksoo maintained members of the UN should be compelled to take action in accordance with Articles 2(4) and 39 of the UN Charter. Furthermore, Aaviksoo highlighted the cyber attacks, when viewed as a use of force, should invoke the collective

self-defense of NATO members against Russia using the provisions of Article 5 of the North Atlantic Treaty (Gurney, 2007).

Unfortunately, prior to the cyber attacks against Estonia, the international community had never considered a united response to the use of force in cyberspace. Following the pleas for action made by Defense Minister Aaviksoo, NATO adopted a cyber defense policy, which set forth general principles and options for NATO and its allies to respond cyber attacks (Hughes, 2009). In addition, the Cooperative Cyber Defense Center of Excellence was established in Estonia as NATO's primary organization for advancing the development of long-term NATO cyber defense doctrine and strategy (Hughes, 2009).

Georgia. In July 2008, the country of Georgia experienced cyber attacks similar in scale, type, and duration to those experienced by Estonia. However, in this case, the cyber attacks appeared to coincide with physical attacks conducted by Russian troops in South Ossetia (Korns & Kastenberg, 2009). According to Markoff (2008), the cyber attacks against Georgia were the first time cyber warfare activities were apparently used as a precursor for and in conjunction with traditional military operations. Similar to the Estonia attacks, Georgian governmental websites were defaced and shutdown by distributed denial of service attacks from a command and control server located within the United States (Markoff, 2008).

Distributed denial of service attacks are conducted when hackers use infiltrated personal computers organized into immense networks (i.e., botnets), infected with malicious programs, to send countless specifically designed requests concurrently to designated websites in order to overload and shutdown targeted servers (Melikishvili,

2008). According to Melikishvili (2008), the July 2008 attacks appeared to be a “dress rehearsal” (para. 5) for the attacks that would accompany the physical attacks in August 2008. While Russian tanks moved into South Ossetia, Georgian government and media websites crashed under what appeared to be a coordinated military operation consisting of kinetic and cyber effects.

The Shadowserver Foundation, a volunteer monitoring organization specializing in detecting, analyzing, and evaluating malicious Internet activities, reported six botnets were used during the Georgian cyber attacks (Melikishvili, 2008). Russian hacktivists were able to overwhelm and shutdown key websites belonging to the President of Georgia, Georgian Parliament, Ministries of Defense and Foreign Affairs, the National Bank of Georgia, and several online news companies (Melikishvili, 2008). Because of these attacks, Korn and Kastenberg (2008) described the Georgian information technology infrastructures as “cyber-locked,” essentially incapable of communicating outside their borders via the Internet. Consequently, the Georgian leadership took the unprecedented step of relocating critical governmental and other official servers to the United States, Estonia, and Poland (Svensson, 2008).

Pentagon. Rosenbach and Klajn (2008) claimed, “America is under silent, but significant, attack” (para. 5). Defense Secretary Gates (2007) said, “The Pentagon sees hundreds of [cyber] attacks a day from a variety of threats” (para. 2). To quantify this assertion, a DHS Report that was accomplished in 2007 found that approximately 13,000 direct cyber attacks were conducted against federal agencies with more than 80,000 attacks on DoD computer networked systems (Rosenbach & Klajn, 2008). Furthermore, DoD officials reported that the military’s global information systems are scanned or

attacked more than 300 million times per day (Rosenbach & Klajn, 2008). The former Director of National Intelligence McConnell added that “[U.S.] information infrastructures . . . increasingly are being targeted for exploitation and potentially for disruption or destruction by a growing array of state and non-state adversaries who have the technical capabilities . . . including Russia and China” (Bruno, 2008, para. 10).

Cyber attacks against Pentagon computer systems have been ongoing for more than 10 years (Baldor, 2009; Starr, 1999). One of the more substantial attacks occurred in 2007, according to Peppler (2007), when more than 1,500 DoD computers were taken offline. Although cyber attacks can originate from state and non-state actors, research has shown that the largest threat to the United States is associated with nation states with advanced cyber warfare capabilities with dedicated programs and the resolve to use cyberspace to achieve political objectives (Report to Congress, 2007). According to Rogers (2008), China and Russia fit into this categorization. Specifically, both China and Russia have made public policy statements about the strategic value of cyber warfare capabilities and the integrated employment of cyber activities as an enabler during the “seize the initiative phase” of armed conflicts (Coleman, 2008b; Mazanec, 2009; Reid, 2007).

In reference to cyber activities, Wright (2008) warned that the United States faces a substantial problem in that Chinese spying continues to increase, and Russian spying has not slowed substantially since the Cold War. China’s vision, according to Reid (2007), is to achieve cyber dominance over its primary rivals (i.e., Great Britain, Russia, South Korea, and United States) by 2050. In support of this goal, Wortzel (2008) reported that China is the most active country with respect to conducting malicious cyber

intrusions. Similar to China, Russia has a robust cyber warfare doctrine designed to be a *force multiplier* used in conjunction with other traditional military activities (Coleman, 2008b). A force multiplier is “a military term that describes a capability that, when added to and employed by a combat force, significantly increases the combat potential of that force” (Fry, 2008, p. 213). Because both China and Russia claim that cyber attacks that originate from IP addresses inside their countries are the acts of rogue hackers and not nation state sanctioned activities, attribution and accountability of such acts are extremely difficult (Bruno, 2008; Mazanec, 2009).

Conclusions

Conclusions derived from an analysis of the literature review are described in this section. Following a summary of historical perspectives, the more substantial findings associated with (a) cyber warfare, (b) decision theory, (c) uncertainty and complexity theories, (d) deterrence theory, and (e) legal aspects are presented. Areas of major agreement and disagreement in the literature are discussed with emphasis on topics of practical significance requiring validation by future research.

Historical perspective. Rona (1976) defined the term “information warfare” in the early 1970s while studying interactions between control systems, a field known as cybernetics. Although information warfare has been in existence since Sun Tzu’s *The Art of War* (Addinall, 2004), Post (1979) introduced the concept of *Cybernetic War* (later shortened to “cyber war”) as the use of computers and the Internet to conduct warfare. In 1984, Gibson coined and defined the term “cyberspace” as an abstract, computerized, global network with *unthinkable complexity*.

More than two decades later, cyberspace was defined within the DoD as a global warfighting domain within the information environment and recognized cyberspace operations as traditional military activities by publishing the first *National Military Strategy for Cyberspace Operations* (England, 2008a, 2008b; Pace, 2006a). With the ever-increasing number of large-scale cyber attacks being conducted against private industries, U.S. critical infrastructures, DoD assets, and nation states, such as Estonia and Georgia, little doubt exists that 21st century warfare will redefine the battlespace and challenge the current doctrine military leaders exercise to make use of force decisions.

Cyber versus traditional warfare operations. The review of the literature showed strong parallels between traditional and cyber warfare operations, activities, and objectives (Hildreth, 2001; Pace, 2006a; Saunders & Levis, 2007). For example, the joint functions of warfare (i.e., command and control, intelligence, fires, movement and maneuver, protection, and sustainment) apply in cyberspace (Pace, 2006a, 2006b; Wilson, 2007b). However, important differences exist. For instance, the decision-maker must consider the dual nature of cyberspace. As a domain, cyberspace is the only domain where warfare and intelligence activities seamlessly comeingle at the atomic and electromagnetic field levels. This duality causes decisional challenges that must be weighed when considering the use of force because military actions in cyberspace can cause adverse effects against legitimate intelligence gathering activities (Butler et al., 2005; Cebrowski, 2002; Wilson, 2007b).

Another difference resides in the concept of determining a valid military target in cyberspace. Because the spectrum of adverse actions in cyberspace ranges from hacking to cyber crime to cyber terrorism to cyber warfare, making the decision to authorize the

use of force following a cyber attack is not as straightforward as traditional warfare (Janczewski & Colarik, 2008). The targeting problem is exacerbated by the inability to achieve unambiguous attribution in cyberspace (Grant, 2007; Saunders & Levis, 2007). Following a cyber attack, the uncertainty created by the lack of attribution creates indecision to exercise the inherent right of self-defense provided by the standing rules of engagement and international law (Schmitt, 1998, 1999; Sharp, 1999a).

Decision theory. With regard to making decisions on the use of force, three decision-making paradigms have emerged as most prevalent. The first is based on von Neumann and Morgenstern's (1944) classical, rational actor model originally proposed to explain economic decisions using expected utility theory (Mintz, Geva, & DeRouen, 1994). With this decision process, the rational actor makes decisions based on maximizing the value of the possible choices within a set of specified constraints. Decision-makers rank the alternatives based on weighted costs and benefits relative to their value system and the situational objectives (Mintz et al., 1994). The decision-maker selects the alternative with the highest expected utility.

The second decision-making paradigm is founded on Steinbruner's (1974) bounded, rational cybernetic model, which refutes the classical, rational assumptions (Mintz et al., 1994). Building on Simon's (1959) earlier work, Steinbruner determined the traditional, expected utility decision theories were not well suited for making use of force decisions. Because "extensive processing time, cognitive effort, concentration, and skills that in many cases are not available, especially under time pressures and rapidly changing conditions," decision-makers rarely maximize utility (Mintz et al., 1994). Consequently, the cybernetic paradigm was designed to address complex and

counterintuitive decisions through an alternative decision structure requiring fewer cognitive and motivational constraints (Ostrom & Job, 1986; Simon, 1959; Steinbruner, 1974). By eliminating possible outcomes not considered feasible, cybernetic decision-making attempts to minimize uncertainty through information feedback loops (Steinbruner, 1974).

Both expected utility and cybernetic decision theories are compensatory theories (Bueno de Mesquita & Lalman, 1990; Ostrom & Job 1986). Therefore, alternatives with a higher valued dimension (e.g., the military use of force) can compensate for a lower valued dimension (e.g., political climate) within the same decision opportunity (Einhorn & Hogarth, 1981). With compensatory models, additive scores of the various alternatives are examined to determine which one maximizes (Bueno de Mesquita & Lalman, 1990) or “satisfies” (Ostrom & Job, 1986) expected utility best. Compensatory models are linear; however, they are often applied in situations in which nonlinear data or characteristics prevail. According to Mintz et al. (1994), the decision to use force is often highly complex due to situational uncertainty and the nonlinear relationships between the competing alternatives. Therefore, noncompensatory decision theories are extremely important to consider when making decisions in multifarious situations in which causal interrelationships are not well defined (Mintz et al., 1994).

The third decision-making paradigm is the poliheuristic, noncompensatory model (Mintz et al., 1994; Mintz, 2004, 2005). Noncompensatory selection procedures are attribute or dimension-based, rather than alternative-based. Alternatives in which the critical dimension falls below a predetermined threshold are removed from consideration. Because compensation between dimensions is not required, heuristics can be used as

“cognitive shortcuts” or experiential “rules of thumb” when making decisions (Tversky & Kahneman, 1974). Thus, noncompensatory models can be more effective in complex decision environments because they are more cognitively manageable (Mintz et al., 1994).

As a different option to expected utility and cybernetic models, poliheuristic approaches are used to simplify complex use of force decisions by leveraging many (“poly”) heuristics (Mintz et al., 1994). According to Mintz (2004), heuristic-based models work particularly well in situations in which one outcome is predominately important. Furthermore, the poliheuristic model of decision-making does not require bounded, rational behavior. Whereas expected utility theory (Bueno de Mesquita & Lalman, 1990) and the cybernetic model (James & Oneal, 1991; Ostrom & Job, 1986) attempt to incorporate political end states when making use of force decisions, both fail to account for the noncompensatory nature of the decision process (Mintz et al., 1994).

Complexity and uncertainty theories. The ubiquitous and invasive nature of the countless interdependent networks that permeate cyberspace necessitates an understanding of complexity theory. Complexity theory is comprised of systems theory, cybernetics, chaos theory, and catastrophe theory. Bennet and Bennet (2008) suggested that complexity theory describes the condition and dynamics of nonlinear systems, situations, or organizations with more elements and relationships than can be understood using normal analytical techniques or logical methods.

According to Schmitt (1997), war is a complex phenomenon comprised of numerous agents who make individual decisions that simultaneously influence the entire system. With the phrase “fog of war,” Clausewitz (1873) described the complexity

warfighters face when making use of force decisions. When developing a decision strategy to use when considering the appropriate response following a cyber attack, the plan should include boundary conditions, tipping points and butterfly effects, stability patterns, equilibrium factors, regenerative feedback loops, and external perturbations (Bennet & Bennet, 2008).

The complexity of war creates a fundamentally uncertain environment (Schmitt, 1997). Therefore, making warfare decisions, such as the use of force, requires an understanding of certainty (i.e., the known), risk (i.e., the unknown), and uncertainty (i.e., the unknowable; Hansson, 2005; Luce & Raiffa, 1957). Although warfighters successfully have applied the MDMP as a deliberate and repeatable methodology during traditional conflicts, this process is too cumbersome for making decisions with the necessary speed and agility to respond to cyber attacks within an adversary's OODA loop (Boyd, 1986; Moffat, 2003). To compensate for the uncertainty associated with cyber warfare decisions, leaders must integrate professional expertise and constant practice with judgment and intuition (Kleindorfer, 2008; Paparone, 2001). Using creative thinking and analysis, commanders exercise *coup d'oeil* (i.e., an "inner light" to see truth through the fog of war) in order to make cyber warfare decisions in which extraordinary complexity and unintended effects are prevalent (Butler et al., 2005; Nicholson, 2005; Schultz, 1997; Vowell, 2004).

Deterrence theory framework. The United States currently does not have a declaratory cyberspace deterrence policy (Gourley, 2008; Kugler, 2009, Taipale, 2009). The challenges of cyber attack attribution and the complexities of potentially harmful and unintended second and third order effects associated with any defensive response action

make establishing a rigid declaratory cyberspace deterrence policy extremely difficult (Gourley, 2008; Taipale, 2009). Given these hurdles, the previous and current presidential administrations have stressed the importance of deterring adverse and hostile acts in cyberspace (Bush, 2003; Obama, 2009). To this end, much work has been devoted to overcoming the technical, social, psychological, and cognitive limitations that prevent applying classical deterrence theory (Brodie, 1946, 1959; Schelling, 1960, 1966) to cyberspace (Barnett, 1998; Chesser, 2007; Kugler, 2009; Taipale, 2009).

Legal aspects of cyber warfare. Three overlapping legal regimes characterize the range of activities in cyberspace: law enforcement, intelligence collection, and military operations (Wingfield & Michael, 2004). Following a cyber attack, the challenge is distinguishing the intruder's legal identity in order to apply the proper legal regime, which determines the range of authorized defense response options (Wingfield & Michael, 2004; Wingfield et al., 2005). Consequently, applying an untailored response following a cyber attack can be unethical, ineffective, or in the worst case, illegal (Peng, Wingfield, et al., 2006; Schmitt, 2002; Sharp, 1999a). Even assuming high confidence attribution, military leaders still require a thorough understanding of the legal aspects of cyber attacks including privacy and civil liberty constraints as well as domestic and international law prior to responding with force (Sharp, 1999a, 1999b; Wingfield & Michael, 2004). To facilitate the decision-making process, Schmitt (1999) proposed a normative framework ("Schmitt Analysis") comprised of the following determinative criteria to be used when evaluating a cyber attack: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.

Limitations and Gaps in the Research Literature

The review of the literature exposed several limitations and research gaps in areas that relate to the uncertainty that military officers encounter when making decisions to use force following a cyber attack. The literature indicated that considerable limitations exist with current U.S. legal and policy frameworks that govern military activities. Specifically, existing laws (both domestic and international) along with associated policies are outdated and do not consider the unique implications of conducting cyber warfare within a global and borderless domain in which the concept of sovereignty is unclear (Owens et al., 2009).

The review of the literature uncovered two important research gaps. First, the predominant military leadership paradigm lacks an understanding of the dimensions and nature of cyber warfare (Butler et al., 2005; Keller & Yang, 2008; Lewis, Langevin, McCaul, Charney, & Raduege, 2008; Pace, 2006a). Specifically, the body of research conducted with regard to DoD transformation and the RMA has not adequately addressed the social, cognitive, behavior, and ethical implications that senior military leaders must consider when making decisions to use force in cyberspace (Bitzinger, 2009; Halpin, Trevorrow, Webb, & Wright, 2006). Second, a lack of research on applying existing decision theories to cyber warfare decision-making processes is evident. Although a considerable amount of research exists regarding how leaders make decisions to use force in response to kinetic attacks within traditional warfighting scenarios, a clear literature gap exists with respect to cyber warfare decision-making theory and processes (Butler et al., 2005; Hansen, 2008; Keller & Yang, 2008; Shen, Chen, Cruz, Blasch, & Kruger, 2007).

National policy and legal frameworks. According to Owens et al. (2009), “Today’s policy and legal framework, for guiding and regulating the U.S. use of cyber attacks, is ill-formed, undeveloped, and highly uncertain” (p. S-3). Furthermore, the conceptual framework that forms the basis of international treaties (e.g., UN Charter, NATO) regarding the use of force and the law of armed conflict does not adequately consider non-state actors or the technical distinctiveness of cyber attacks (Joyner & Lotrionte, 2001; Kennedy, 2006; Wingfield, 2007, 2009). Because cyber attacks potentially will have detrimental impact on U.S. private industries and international partners, the need for robust coordination and deconfliction processes along with civil liberty policies are required for synchronizing cyberspace operations (Carafano & Weitz, 2008; Owens et al., 2009; Wilson, 2008).

Although the U.S. Congress has specific responsibilities when authorizing the use of force, Owens et al. (2009) argued, “The contours of that authority and the circumstances under which authorization is necessary are at least as uncertain for cyber attack as for the use of other weapons” (p. S-5). In addition, the considerations for developing and applying the appropriate standing rules of engagement for cyber attacks are extremely complex, which adversely affect a commander’s ability to execute the inherent right of self-defense (Kelsey, 2008; Saunders & Levis, 2007). Last, the United States does not have a clear declaratory policy for deterring cyber attacks (Gourley, 2007; Libicki, 2009; Taipale, 2009). This policy limitation primarily results from the lack of a credible deterrence model for cyberspace; the challenges associated with attribution; and the absence of cyber attack severity thresholds (Kugler, 2009; Taipale, 2009).

Leadership paradigms. The transformational thinking that has accompanied the RMA has not caused a shift in the traditional warfighting paradigm (Bitzinger, 2009; Halpin et al., 2006). The review of the literature showed a research gap exists with respect to generalizing existing leadership theories to account for the unique challenges encountered within the ubiquitous and collaborative nature of cyberspace. Specifically, the literature indicates senior military officers are making decisions about the use of force in cyberspace within a paradigm founded on traditional and outdated ideologies of warfare (Butler et al., 2005; Keller & Yang, 2008; Pace, 2006a). According to Owens et al. (2009), conducting cyber attacks stresses the “existing ethical and human right regimes” (p. S-4) in a manner that is not adequately addressed in the literature. Consequently, the moral and ethical principles that underlie the law of armed conflict have not been applied rigorously to cyber attacks (D. Denning, 2007; Wingfield, 2009). Therefore, translating the concepts of proportionality, necessity, distinction, and chivalry to cyber warfare activities is extremely difficult but essential for authorizing the use of force (Kelsey, 2008; Peng, Wijesekera, Wingfield, & Michael, 2006; Wingfield, 2007, 2009).

Pace (2006a) argued that leaders require a better understanding of the social, behavioral, and cultural aspects of cyberspace on a global scale in order to conduct cyber warfare activities successfully. Understanding the dynamic, complex, and interrelated effects associated with cyber attacks requires trained leaders capable of judging the policy, legal, and ethical significance of such attacks with an insight into an adversary’s intent or motivation (D. Denning, 2007; Kennedy, 2006; Pfister & Böhm, 2008). These issues are not addressed adequately in the literature. Furthermore, the literature review

showed that professional development and educational curricula changes are needed to improve cyber warfare expertise (Carafano & Weitz, 2008; Hansen, 2008; Kramer et al., 2007; Pace, 2006a).

Decision-Making processes. The review of the literature indicated an apparent gap regarding the application of existing decision theory to cyber warfare decision processes. Owens et al. (2009) asserted, “The decision-making apparatus for cyber attack and the oversight mechanisms for that apparatus are inadequate today” (p. S-4). Furthermore, Wingfield (2007) noted that the effects and unintended consequences of cyber attacks are likely to be more uncertain than the predictable outcomes for traditional kinetic attacks. Noting the clear lack of research in this area, Owens et al. proposed a national debate should be stimulated to determine a “clear, transparent, and inclusive decision-making structure . . . to decide how, when, and why a cyber attack should be conducted” (p. S-5).

The prevailing decision theories associated with the use of force (e.g., expected utility, cybernetic, and poliheuristic) have assumptions and ranges of applicability that have not been validated with making cyber attack decisions (Keller & Yang, 2008; Shen et al., 2007). Furthermore, the established MDMP is based on a deliberative and systematic sequence of steps not designed or equipped for making rapid (at network speeds) response decisions in cyberspace (Hansen, 2008). Research gaps exist on developing new decision-making models (e.g., Boyd’s [1986] “OODA Loop”) that include the ability to integrate real time considerations of policy and legal constraints, current diplomatic environment, in addition to law enforcement and intelligence

community activities in sufficient detail to provide decision-makers a comprehensive understanding of these interrelated components (Butler et al., 2005; Owens et al., 2009).

Summary

Chapter 2 included a review of the literature associated with cyber warfare, decision-making processes, and the phenomenon of uncertainty. Following a historical perspective (Addinall, 2004; England, 2008a, 2008b; Gibson, 1984; Pace, 2006a; Post, 1979), an exploration of the similarities and differences between cyber warfare activities and traditional warfare operations was presented (Butler et al., 2005; Cebrowski, 2002; Grant, 2007; Hildreth, 2001; Janczewski & Colarik, 2008; Pace, 2006a, 2006b; Saunders & Levis, 2007; Schmitt, 1998, 1999; Sharp, 1999a; Wilson, 2007b). Compensatory (expected utility and cybernetic) and non-compensatory (poliheuristic) decision theories (Bueno de Mesquita & Lalman, 1990; Einhorn & Hogarth 1981; Geva, & Derouen, 1994; James & Oneal, 1991; Mintz, 2004, 2005; Mintz et al., 1994; Ostrom & Job, 1986; Simon, 1959; Steinbruner, 1974; Tversky & Kahneman, 1974; von Neumann & Morgenstern, 1944) were shown to form the most developed theoretical framework for making decisions to use force in complex environments such as cyberspace.

The review of the literature indicated that complexity and uncertainty theories (Bennet & Bennet, 2008; Boyd, 1986; Butler et al., 2005; Hansson, 2005; Kleindorfer, 2008; Luce & Raiffa, 1957; Moffat, 2003; Nicholson, 2005; Paparone, 2001; Schmitt, 1997; Schultz, 1997; Vowell, 2004) that normally apply to complex systems are capable of describing phenomena in cyberspace. Although the United States does not currently have a declaratory cyberspace deterrence policy (Bush, 2003; Obama, 2009; Taipale, 2009), the review of the literature showed classical deterrence theory frameworks

(Brodie, 1959; Schelling, 1960, 1966) and cyberpower theories (Jordan, 1999; Kramer et al., 2007) are being used to develop a comprehensive cyber deterrence strategy (Barnett, 1998; Chesser, 2007; Gourley, 2008; Kugler, 2009). Finally, a thorough examination of the legal aspects of cyber warfare (Peng, Wingfield, et al., 2006; Schmitt, 1998, 1999, 2002; Sharp, 1999a; Wingfield & Michael, 2004; Wingfield et al., 2005) indicated decision-makers face complex challenges in three overlapping legal regimes.

Chapter 3 includes a description of the methodology and design selected for this research study including an explanation of the design appropriateness. In addition, the research question, population, sampling frame, and the informed consent process are presented. Following a discussion of the validity and reliability considerations, the data collection and analysis procedures are described. Chapter 3 is concluded with a summary of the information presented.

Chapter 3: Method

The purpose of this qualitative, phenomenological research study was to explore the decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack. A qualitative research method is used when exploring meaning or discovering understanding of a central phenomenon (Creswell, 2007; Neuman, 2005). Qualitative research is the preferred method when studying leadership phenomena such as decision-making uncertainty (Bryman et al., 1988; Conger, 1998; Yukl, 1989). Eldabi et al. (2002) added that qualitative research should be used when the goal of the study is to understand the contextual and experiential elements of a complex situation, process, or interaction when a governing model does not exist. Furthermore, qualitative methods are appropriate when a study is used to describe, understand, and answer questions about the nature of a central phenomenon from the perspectives and lived experiences of participants by inductively analyzing the rich data collected in their natural setting (Bryman, 1984; Leedy & Ormrod, 2010; Neuman, 2005).

A phenomenological design was used in this qualitative research study. Phenomenological research is used to seek understanding of an individual's subjective perceptions and the meaning of lived experiences (Giorgi, 2006; Moustakas, 1994; van Manen, 1990). Mertens (2005) suggested, "The feature that distinguishes phenomenological research from other qualitative research approaches is that the subjective experience is at the center of the inquiry" (p. 240). The intent is to understand and describe a phenomenon "from the point of view of the participant" (Mertens, 2005, p. 240). Phenomenological research designs are most effective at exposing, describing, and developing individual experiences and perceptions based on the research participants'

insights and lived experiences (Donalek, 2004). In comparison to other qualitative research designs, phenomenological research is particularly effective when exploring the lived experiences associated with decision-making under uncertainty (Donalek, 2004; Gilstrap, 2007; Goulding, 2005; Mitroff & Sagasti, 1973; Starks & Trinidad, 2007).

For this qualitative, phenomenological study, semi-structured, taped, and transcribed interviews with senior military officers were used to explore and understand their perceptions and lived experiences associated with the decision-making uncertainty when determining the response to a cyber attack (Groenewald, 2004; Kvale, 1996; Moustakas, 1994). The specific population group in this study was senior military officers serving as members of the Joint Chiefs of Staff (JCS) who make cyber warfare decisions. The senior military officers who were interviewed were stationed at the Pentagon in Washington, DC. The phenomenological reduction process employed Moustakas' modification to van Kaam's (1959, 1966) method of qualitative data analysis. The experiential narrative data collected from the participants were analyzed for key themes, common patterns, and units of meaning using QSR[®] NVivo 8 software (Groenewald, 2004; QSR International, 2007).

The purpose of chapter 3 is to discuss the research methodology and design identified for the study including the appropriateness of the selected approach in comparison to other research methods and designs considered. In addition, a description of the research question, the population, and the sampling frame including the methods used to ensure confidentiality and to obtain informed consent is presented. A discussion of the study's geographic location, instrumentation reliability and validity, data collection, and data analysis completes the chapter.

Research Method

A qualitative method was used to explore the central phenomenon of decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack. According to Leedy and Ormrod (2010), qualitative research methods “. . . focus on phenomena that occur in natural settings . . . and involve studying those phenomena in all their complexity” (p. 135). Qualitative approaches are preferred for studying human events (e.g., interpersonal relationships and social interactions) and cognitive processes (e.g., perception, intuition, reasoning, and judgment; Creswell, 2009; Langdridge, 2008; Leedy & Ormrod, 2010). Decision-making is a complex cognitive process that integrates experience with intuition, perceptions, and heuristics to construct judgments (Cioffi, 1997; Cohen et al., 2008; Dane & Pratt, 2007). Therefore, qualitative research methods are recommended when studying leadership phenomena such as decision-making uncertainty (Bryman et al., 1988; Conger, 1998; Eldabi et al., 2002; Yukl, 1989).

Several characteristics made qualitative methods preferred over quantitative methods for this research study. Holosko (2006) proposed six comparisons that assist the researcher with selecting the most appropriate research method. First, the research study’s goals and objectives should dictate the research method used (Creswell, 2009; Leedy & Ormrod, 2010; Holosko, 2006; Neuman, 2005). For this study, the research goal was to understand the lived experiences and perceptions of senior military officers following a cyber attack. Qualitative methods are designed to understand individuals and events in natural settings (Holosko, 2006; Leedy & Ormrod, 2010). Second, the epistemological perspective should be considered. Qualitative research is primarily

interpretive whereas quantitative research is mainly positivistic (Bryman, 1984; Dobrovolny & Fuentes, 2008; Holosko, 2006).

This qualitative study was part of the interpretive paradigm (seeking to understand) and employed transcendental phenomenology (essence of experiences emerging into consciousness) to explore the decision-making experiences as described by senior military officers. Burrell and Morgan (1979) described interpretive theory as “the study of ways in which social reality is meaningfully constructed and ordered from the point of view of the actors directly involved” (p. 254). Reality is individually and socially constructed (Berger & Luckmann, 1966; Schutz, 1967). Interpretive researchers seek to understand experiences not apparent through positivistic (empirical) methods of inquiry (Burrell & Morgan, 1979). Furthermore, interpretivists seek to “explain the stability of behavior from the individual’s viewpoint” (Burrell & Morgan, 1979, p. 254) through intersubjective processes.

Logical orientation is the third characteristic that Holosko (2006) recommended researchers use to select the appropriate research method. Qualitative research is an *inductive* process that explores a problem by proceeding from “a general point of view to a specific conclusion . . . or grounded theory” (Holosko, 2006, p. 13). In contrast, quantitative research is a *hypothetico-deductive* process that begins with a specific theory and forms generalizable conclusions (Cassell, Buehring, Symon, & Johnson, 2006; Creswell, 2005; Holosko, 2006). The current study was used to explore the separate experiences and perceptions of individual participants with the goal of discovering common themes and constructing a composite description of the decision-making

uncertainty phenomenon. Therefore, the logical orientation of the inductive process was followed in this study.

The fourth consideration researchers should evaluate when determining the research methodology is the level of dynamism (Holosko, 2006). For qualitative methods, researchers must immerse themselves into the natural setting and become an integral part of the participant's experiential perspective (Holosko, 2006; Ospina, 2004). To the maximum extent possible, the immersion process is necessary for collecting rich, contextual, and descriptive data.

Quantitative methods employ a more rigid, deterministic process: problem statement, assumptions, hypotheses, data collection, statistical tests, and conclusions (Creswell, 2009; Holosko, 2006; Leedy & Ormrod, 2010). Therefore, with quantitative methods, the researcher is much more detached from the participants and focused primarily on following the linear steps of the scientific method and hypothesis testing procedure (Dobrovolny & Fuentes, 2008). Because of the nascent and complex nature of the phenomenon under investigation in the current study, the collection of highly descriptive and contextual narratives was necessitated in order to understand the lived experiences and perceptions of a limited number of participants.

The fifth characteristic that distinguishes qualitative from quantitative methods is the use and generation of theory (Blum & Muirhead, 2005; Holosko, 2006). In qualitative methods, the use of theory to frame the study is not initially required (Creswell, 2007; Holosko, 2006). To this assertion, many qualitative researchers argue that presupposing the governing theory and rigorously defining exact research questions and hypotheses may unnecessarily delimit their study (Creswell, 2005, 2007; Holosko,

2006). In addition, qualitative research often results in a “simple explanatory or middle-range theory, referred to as grounded theory” (Holosko, 2006, p. 13).

In comparison, quantitative theory begins with relevant theory as the basis for deriving testable assumptions and hypotheses (Bryman, 1984; Creswell, 2007; Smith, 1983). The data collected in quantitative studies are used to verify or refute the base theory from which the hypotheses were formulated. For this research study, the review of the literature showed no single theory exists for the phenomenon under study (Bartholomees, 2008; Czerwinski, 1998; DeRouen, 2000; Hansson, 2005; Schultz, 1997; Yukl, 1989). Therefore, qualitative methods were more appropriate for studying a phenomenon of this complexity (Eldabi et al., 2002).

The sixth and final characteristic that should be evaluated when determining the proper research method concerns the researcher’s role during the data collection process (Creswell, 2007; Holosko, 2006; Smith, 1983). When conducting qualitative research, the “researcher is the instrument” (Patton, 2002, p. 14). Specifically, for qualitative methods, the “*sine qua non* is a commitment to see the world from the point of view of the actor” (Bryman, 1984, p. 77). Therefore, the researcher is actively engaged and immersed in the natural environment being studied while the data are collected from *participants* (Dobrovolny & Fuentes, 2008; Holosko, 2006).

In contrast, quantitative methods have no such requirement for the researcher to be immersed in the natural environment. In general, the researcher conducting a quantitative study has a passive, separated, and often detached role from the research *subjects* (Bryman, 1984; Dobrovolny & Fuentes, 2008; Holosko, 2006). The resulting outcome of quantitative research is an impersonal, objective report of the research

findings displayed using numerical and graphical methods (Dobrovolny & Fuentes, 2008). For this study, the goal was to create a participant-observer role using qualitative methods in which lived experiences and perceptions were explored using “induction to analyze collected data (e.g., code interview transcripts, identify themes and patterns)” (Dobrovolny & Fuentes, 2008, p. 9).

Cooper and Schindler (2008) submitted, “Qualitative refers to the meaning, the definition or analogy or model or metaphor characterizing something, while quantitative assumes the meaning and refers to a measure of it” (pp. 146-147). Quantitative research methods are designed to “measure variables . . . of the physical world or carefully designed measures of psychological characteristics or behaviors” (Leedy & Ormrod, 2010, p. 94) by collecting numerical data and using statistical procedures to analyze and deduce conclusions from the given data. In addition, quantitative research studies can show correlations between variables that can be generalized from a sample to a defined population (Creswell, 2009; Dobrovolny & Fuentes, 2008). However, the nature of the research question, the complexity of the central phenomenon, the lack of a coherent theoretical framework, the paucity of supporting literature, and the desire to explore the lived experiences and perceptions of the participants, made quantitative methods inappropriate for this research study for several reasons (Creswell, 2009; Dobrovolny & Fuentes, 2008; Leedy & Ormrod, 2010).

First, the number of individuals with considerable cyber warfare decision-making experience is extremely limited. Therefore, the sample would not have been statistically significant and the results would have been prone to large standard errors. Second, the number of cyber attacks detrimental enough to consider the use of force is also limited.

Accordingly, insufficient data were available to analyze variables such as the Schmitt (1999) cyber attack parameters (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility) for trends, correlations, and hypotheses testing. Last, quantitative designs did not permit the rich open-ended discussion capable of stimulating the individual experiences and perceptions of senior military officers who make cyber warfare decisions. As a result, phenomenological studies were conducted to capture the “essence of human experiences . . . as described by the participants in the study” (Creswell, 2007, p. 15). Therefore, qualitative research methods are best when seeking to gain a deeper understanding of multiple realities (Lincoln & Guba, 1985).

In contrast to quantitative research, which has specific sampling requirements, sampling in qualitative research is purposeful and exhausted when no new themes emerge from the data (Creswell, 2005; Lincoln & Guba, 1985). Seidman (2006) identified two criteria that researchers should aim for: (a) proper representation of the population and (b) saturation of information. Saturation, according to Creswell (2005), is the “point where you have identified the major themes and no new information can add to your list of themes or to the detail for existing themes” (p. 244). Avoiding a commitment to a specific number, Seidman defined “enough” as the point at which the study participants begin to share the same information in combination with other practical criteria such as availability of time, money, and other resources. Based on historical averages for qualitative studies cited in the literature (Boyd, 2001; Creswell, 2007; Luborsky & Rubenstein, 1995), this research study was estimated to require approximately 20 participants to reach thematic saturation.

Typically, purposeful (representative) sampling is used for qualitative research (Creswell, 2005). In purposeful sampling, Creswell (2005) noted, “Researchers intentionally select individuals and sites to learn or understand the central phenomenon” (p. 204). The standard used when choosing participants, according to Patton (2002), is they are “information rich” (p. 230). For this study, the participants were senior military officers with considerable experience making traditional and cyber warfare decisions. Personal interviews were conducted with senior military officers who served for the CJCS and who were screened specifically for their experience and performance prior to assignment. Because the participants worked within the DoD Headquarters at the Pentagon in Washington, DC, they were exposed to cyber warfare events, situations, and conflicts at the national level. The participants in this study served as the primary source data. Secondary source data included personal communications, books, scholarly journals, and doctoral dissertations.

Appropriateness of Design

For this qualitative research study, a phenomenological design was used to explore the lived experiences and perceptions of senior military officers following a cyber attack. Based on a comparative evaluation, phenomenology was the most appropriate qualitative research design compared to other research designs considered for this study. Phenomenology, a term first used in philosophical writings by Kant as early as 1764, is derived from the Greek word *phainein*, meaning to appear, to flare up, or to show itself (Priest, 2002). Following Kant’s work, Hegel formalized the meaning of phenomenology in 1807 as the knowledge that emerges from consciousness and perceptual awareness (Dowling, 2007; Moustakas, 1994).

Although Kant (1764) and Hegel (1807) first recognized the importance of phenomenology as a philosophical concept, Brentano (1838-1917) is credited in the literature with inspiring Husserl by relating “descriptive psychology” to “descriptive phenomenology” (Dowling, 2007). A German mathematician and logician, Husserl (1859-1938) is attributed with developing the conceptual framework of transcendental phenomenology (Dowling, 2007; Moustakas, 1994; Priest, 2002; van Manen, 1990). Husserl’s objective was “to discover the nature, goals, and methods of philosophical inquiry” (Priest, 2002, p. 51).

Phenomenology is the study of lived experiences as described by individuals who experienced the phenomena (Burrell & Morgan, 1979; Husserl & Welton, 1999; Moustakas, 1994; Schutz, 1967). According to Moustakas (1994), Husserl embraced Bertano’s notion of *intentionality* as the “fundamental concept for understanding and classifying conscious acts and experiential mental practices” (Dowling, 2007, p. 132). Husserl also recognized *intuition* as a key concept of transcendental phenomenology (Moustakas, 1994). In this context, Husserl adopted Descartes’ (1644/1983) interpretation of intuition as “an inborn talent directed toward producing solid and true judgments concerning everything that presents itself” (p. 22). Therefore, the essence of Husserl’s (1931) phenomenological theory is intentionality and intuition manifested through the ability to make judgments as knowledge emerges to consciousness (Moustakas, 1994).

Transcendental phenomenology, as a method of inquiry, is a structured process of understanding a central phenomenon as described by the participants (Moustakas, 1994). The objective of this study was to understand the experiential essence of cyber warfare

decision-making uncertainty as described by senior military officers. This research goal was achieved by using *phenomenological reduction* to facilitate the transcendence and description of the participants' experiences through interpretive understanding (Priest, 2002). The term *reduction* in this context means the researcher uses interpretive skills to "reduce the world as it is considered in the natural attitude to a world of pure phenomenon or . . . to a purely phenomenal realm" (Dowling, 2007, p. 132).

Of the more prevalent traditions of qualitative research described by Creswell (2007), Bednall (2006) contended, "Phenomenology relies on the interpretative legitimacy of the researcher" (p. 2). To ensure legitimacy during phenomenological research, the researcher must depart from the *natural attitude* of preexisting knowledge and judgments by exhibiting epoché (Dowling, 2007). Epoché, according to Dowling (2007), is "a Greek word meaning to refrain from judgment or stay away from everyday, commonplace way of perceiving things" (p. 132). Moustakas (1994) asserted that Husserlian transcendental phenomenology is distinguished by its pureness because biases and preconceived notions are bracketed, or set aside, in an attempt to consider the data as purely as possible. Although impossible to eliminate all sources of bias, undesired effects are minimized by employing epoché and bracketing processes. Epoché and bracketing were used to acknowledge and set aside biases during the interview and data analysis processes (Bednall, 2006; Langdridge, 2008).

Phenomenological research designs are particularly well suited for exploring decision-making experiences (Anderson & Eppard, 1998; Donalek, 2004; Karlsson, 1992; Starks & Trinidad, 2007). This assertion is based on the similarities between the epistemological principles fundamental to phenomenology and decision-making

(Karlsson, 1992; Mitroff & Sagasti, 1973). Specifically, phenomenology is founded on the premise that experience is the primary source of knowledge through the lens of intentionality and intuition (Husserl, 1931; Moustakas, 1994; Priest, 2002). Similarly, Pace (2006b) wrote, “Effective decision-making combines judgment and intuition acquired from experience, training, study, and creative thinking. Commanders visualize the situation and make sound and timely decisions” (p. III-2). Decision-making is a complex process occurring along a spectrum of certainty in which probability distributions, experience, intuition, rationality, risk acceptance, beliefs, and values factor into the decision calculus (Bennet & Bennet, 2008; Böhm & Brun, 2008; Vowell, 2004).

Karlsson (1992) conducted a formal comparison of phenomenology and decision-making using a cognitive information-processing paradigm. Essential to this evaluation is the concept of *intentionality*. A fundamental principle of phenomenology, intentionality is the most basic structure of consciousness and implies that all perceptions have meaning (Dowling, 2007; Husserl, 1931; Karlsson, 1992). Intentionality is the internal experience of being conscious about something (Moustakas, 1994; van Manen, 1990). Based on this understanding, Karlsson argued that decision-making is an outward manifestation of intentionality at the epistemological level.

Karlsson (1992) added that phenomenological and decision-making processes share similar cognitive operations. In both cases, experiences and knowledge-based perceptions are leveraged to make judgments between thematic alternatives as a means of creating a projected future (Karlsson, 1992). Karlsson defined a projected future as “a subjective determination of future realizable possibilities” (p. 422). Whereas phenomenology is used to seek understanding of the essence of a phenomenon by

describing lived experiences, for decision-making, lived experiences are used to act on the essential structure of the phenomenon. However, in both cases, the cognitive process relies on intentionality and intuition to allow the essence of the phenomenon to emerge (Dowling, 2007; Moustakas, 1994; Priest, 2002).

Giorgi (2006) found that many variations of Husserlian phenomenology exist among the more prominent phenomenological research psychologists. Specifically, Giorgi conducted an analysis of the phenomenological designs published by Colaizzi (1978), Giorgi (1985), Hycner (1985), Karlsson (1993), Moustakas (1994), and van Manen (1990). Although several differences were found between each design using phenomenological criteria, Giorgi (2006) asserted the key similarities were founded on understanding the “phenomenon being experienced and not . . . the particular individual who is experiencing the phenomenon” (p. 318). For this study, the research design was primarily centered on Moustakas’ interpretation of Husserl’s phenomenology including the modified van Kaam (1959) method of data analysis.

Other Qualitative Research Designs Considered

Ethnography is the use of fieldwork within a social setting to observe the direct activities of a group under study, including their behaviors, communications, and interactions (Creswell, 2007; Goulding, 2005; Wolcott, 1994). Based on foundational work by Malinowski and Mead in cultural anthropology, Van Maanen (1988) observed, “The result of ethnographic inquiry is cultural description . . . a description of the sort that can emerge only from a lengthy period of intimate study and residence in a given social setting” (p. 103). Ethnographic designs, according to Creswell (2005), are qualitative research procedures for “describing, analyzing, and interpreting a culture-

sharing group's shared patterns of behavior, beliefs, and language that develop over time" (p. 436). Central to this premise is how Creswell defined culture as "everything having to do with human behavior and belief" (p. 436).

Ethnographic research "typically includes a study of the group's history, geography, kinship patterns, structures, functions, rituals, symbols, politics, economic factors, educational and socialization systems, and the degree of contact between the target and mainstream cultures" (Mertens, 2005, p. 234). Creswell (2005) proposed ethnographies should be conducted when studying a population that shares the same culture as developed from common values, beliefs, and language. Goulding (2005) noted that the ethnographic design is best suited for studying organizational culture and power dynamics in which the main source of data collection is through prolonged participation and direct observation. Atkinson, Coffey, and Delamont (2003) stressed that firsthand observation and participation within the social setting are essential for the researcher to understand the participants under study and evaluation.

An ethnographic design was not appropriate for this research study. First, observing the decision-making uncertainty that senior military officers experience following a cyber attack was not logistically feasible. Because cyber attacks are discrete and unpredictable events that occur without notice, conducting direct observation fieldwork was not realistic. Furthermore, the decisional process following a cyber attack occurs in different locations within the Pentagon based on the attack's characteristics and effects. Therefore, the ability to predict the observation location accurately was highly unlikely. Last, the purpose of this study was to gain an understanding of the individual lived experiences and perceptions of senior military officers following a cyber attack

without preconceived causality. Therefore, using an ethnographic inquiry might have inappropriately inferred the decisional experiences were associated with a particular belief system, social setting, or cultural interaction.

A case study is “an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident” (Yin, 2009, p. 18). The case study design, according to Yin (2009), is preferred for research studies that are designed to explain “how” or “why” a particular phenomenon occurs based on an “extensive and in-depth description” (p. 4) of the phenomenon. Furthermore, Yin asserted that case study inquiry “relies on multiple sources of evidence, with data needing to converge in a triangulating fashion” (p. 18). A case study is an “in-depth exploration of a bounded system (e.g., an activity, event, process, or individuals) based on extensive data collection” (Creswell, 2005, p. 439). According to Mertens (2005), a case study is “a method for learning about a complex instance, based on a comprehensive understanding . . . obtained by extensive descriptions and analysis of that instance taken as a whole and in its context” (p. 237).

Although many authors consider a case study as a special type of ethnography, Creswell (2005) maintained case studies differ from ethnographies in several important ways. Specifically, case study researchers often focus on a program, event, or activity involving individuals rather than a group per se (Stake, 1995, 2000). In addition, case studies are used frequently to describe the “activities of the group instead of identifying shared patterns of behavior exhibited by the group” (Creswell, 2005, p. 439). With this in mind, Yin (2009) noted that a primary limitation of the case study design is the

inability to generalize the findings obtained from studying individual actions to understanding the potential outcomes of the collective group.

The case study design was inappropriate for this research study for several reasons. Schramm (1971) wrote, “The essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a *decision* or set of decisions: why they were taken, how they were implemented, and with what result” (p. 21). However, this study was designed to explore decision-making uncertainty following a cyber attack by understanding the lived experiences and perceptions of senior military officers. Therefore, the goal was not to understand why or how particular decisions were made to achieve a specific end state. Although individual interviews were used to collect data for this study, key themes emerged that were common among senior military officers as a collective group of the Joint Staff. The case study design is limited in extracting these communal behaviors and experiences (Stake, 1995; Yin, 2009).

Because the specific details and analysis parameters associated with actual cyber attack cases contain highly classified information, a case study’s findings would not have been releasable or publishable (Wilson, 2007b). Furthermore, this study was designed to improve the understanding of the decisional uncertainty experienced by senior military officers following cyber attacks of various severities and intensities. Therefore, using the case study approach to research a particular, unclassified cyber attack unnecessarily limited the scope of this understanding.

The next qualitative research design considered for this research study was the Delphi technique. The Delphi technique “may be characterized as a method for structuring a group communication process so that the process is effective in allowing a

group of individuals, as a whole, to deal with a complex problem” (Linstone & Turoff, 1975, p. 3). The Rand Corporation originally developed the Delphi technique in the 1950s as a method of reducing the adverse effects of interpersonal interactions during group decision-making and forecasting processes (Goodman, 1987; Hasson, Keeney, & McKenna, 2000). According to Linstone and Turoff (1975), the objective of the original design was “to obtain the most reliable consensus of opinion of a group of experts . . . by a series of intensive questionnaires interspersed with controlled opinion feedback” (p. 10). Over time, the Delphi technique matured to a group facilitation process that uses a multistage, iterative process designed to convert opinion to group consensus with the goal of developing a forecast, policy, or decision (Goodman, 1987; Grisham, 2009; Hasson et al., 2000).

Goodman (1987) found that four features distinguish the Delphi technique from other group decision-making processes. These characteristics are “anonymity, iteration with controlled feedback, statistical group response, and expert input” (Goodman, 1987, p. 729). With each iterative round, Linstone and Turoff (1975) noted the validity of the resulting judgment is measured by the “degree of consensus” between the experts. In this context, consensus is the convergence of opinion and not complete agreement (Goodman, 1987). A generally accepted definition of consensus does not exist for the Delphi technique (Hasson et al., 2000; Linstone & Turoff, 1975). Whereas the range of consensus in the literature ranges from 51% to 80%, Hasson et al. (2000) argued a better measurement of consensus is the stability of the responses.

Although the Delphi technique is designed to reach consensus in response to a complex problem, several important considerations made this research design

inappropriate for this research study. First, the purpose of this study was to explore the lived experiences and perceptions of senior military officers and not to develop a decision or create a new policy about cyber warfare. Second, senior military officers comprised the population for this study. Even though the officers are experts in cyber warfighting doctrine, they are not necessarily experts in decision theory, uncertainty theory, or the technical aspects of a cyber attack (Linstone & Turoff, 1975). Therefore, assembling a group of *experts* based on meaningful criteria and suitable for answering complex questions regarding decision-making uncertainty would not have been achievable or defensible using the desired population (Rowe and Wright, 1999). Finally, existing policy prohibits Joint Staff members from developing a decision or policy for unofficial purposes that could be construed to reflect the opinion of the Joint Staff, the DoD, or a particular military department (D. A. Armstrong, personal communication, January 13, 2009).

Grounded theory was the final qualitative design considered for this research study. Developed with origins in sociology, the main objective of a grounded theory research design is to develop an explanatory theory of a social process that occurs within its natural environment (Glaser & Strauss, 1967). Strauss and Corbin (1994) defined grounded theory as “a general methodology for developing theory that is grounded in data systematically gathered and analyzed” (p. 273). Using comparative analysis, grounded theory research “enables one to generate a broad theory about a qualitative central phenomenon *grounded* in the data” (Creswell, 2005, p. 395). Grounded theory research is a “process theory” design used to explain experiences, perceptions, activities,

and interactions that evolve over time (Creswell, 2005; Starks & Trinidad, 2007; Strauss & Corbin, 1990).

Creswell (2005) asserted that one uses grounded theory when a “broad theory or explanation of a process . . . is desired that fits a particular situation, actually works in practice, is sensitive to individuals in a setting, and may represent all of the complexities actually found in the process” (p. 396). In order to characterize the complexities found in the process under study, grounded theory requires a substantial data collection effort with availability to many more participants than typically required for other qualitative research methods (Creswell, 2005). To this assertion, Goulding (2005) noted grounded theory research designs require conducting the study in “a variety of contexts, ensuring full theoretical sampling and the production of a theory that has applications to other settings and populations” (p. 298). Consequently, the data collection and interpretation efforts that are required to reach theoretical saturation are considerable and frequently unpredictable (Charmaz, 2006; Goulding, 2005).

A grounded theory design was inappropriate for this research study. First, the purpose of this study was to explore the lived experiences and perceptions of senior military officers following a cyber attack and not to develop a process theory that explains actions or activities associated with the central phenomenon. Second, grounded theory as a research design “. . . was developed for, and is particularly suited to, the study of behavior” (Goulding, 1998, p. 56). However, the key themes and invariant constituents that emerged from exploring the lived experiences and perceptions associated with decision-making uncertainty were not necessarily caused by the participant’s behavior. Specifically, decision-making uncertainty in cyber warfare is a

function of many other factors such as social, cultural, cognitive, technical, and ethical aspects (Aiello, 2008; Borgmann, 2004; Pace, 2006a; Rowe, 2007). Using phenomenology allowed these areas to be explored fully without this design limitation.

The next concern with a grounded theory approach was associated with the coding procedure. Strauss and Corbin (1990) added an additional coding step to the grounded theory comparative analysis procedure originally developed by Glaser and Strauss (1967). This step, known as *axial coding*, was placed between the initial *open* and final *theoretical* coding steps as a means of facilitating the process. During the axial coding process, researchers place all open-coded data into six predetermined categories: causal conditions, phenomena, context, intervening conditions, actions/interaction strategies, and consequences (Strauss & Corbin, 1990). Unfortunately, critics of the axial coding process assert the intermediate step is unnecessarily restrictive and artificially limits the exploration to the six predetermined categories of the Strauss and Corbin paradigm model (Glaser, 1992; Hall & Callery, 2001; Kendall, 1999).

The final concern with grounded theory was associated with the data collection requirements to reach theoretical saturation. As described earlier, a substantial number of participants often are required for grounded theory research in comparison to other qualitative research designs (Charmaz, 2006; Creswell, 2005; Goulding, 1998, 2005). Because the number of senior military officers with credible cyber warfare experience assigned to the Joint Staff is limited to approximately 30, the potential existed that the number of willing participants would have been exhausted prior to a new theory emerging from the collected data. Therefore, considering the four concerns presented above, grounded theory research was inappropriate for this research study.

Research Question

Gaining a better understanding of the decision-making uncertainty encountered by senior military officers following a cyber attack through their perceptions and lived experiences was the focus of this study. Moustakas (1994) found the development of a research question that has “social and personal significance” (p. 104) to be essential to conducting phenomenological research. In addition, Moustakas noted, “The [research] question must be stated in clear and concrete terms . . . so that the intent and purpose of the investigation are evident” (p. 104). To explore the identified phenomenon while facilitating the reflection of the experiential descriptions, this study was guided by the following research question: *How do senior military officers perceive and describe the lived experience of decision-making uncertainty when determining the appropriate response to a cyber attack?*

The research question was open-ended and non-directional in order to obtain the lived experiences of the research participants in an environment that minimized researcher bias and encouraged the identification of alternative perspectives. The intent was to “reveal more fully the essences and meanings” of the “comprehensive descriptions . . . and accurate renderings of the experience” by engaging the “total self of the research participant” (Moustakas, 1994, p. 105). Leedy and Ormrod (2010) noted, “Qualitative researchers construct interpretive narratives from their data and try to capture the complexity of the phenomenon under study” (p. 103). The lived experiences and perceptions of senior military officers serving on the Joint Staff specifically assigned to cyber divisions who have extensive experience making cyber warfare decisions were explored in this research study.

Population

According to Cooper and Schindler (2008), identifying the target population (i.e., people, events, or records that can answer the research questions) is an essential step when designing the research study. The target population for this study was senior military officers assigned to cyber divisions on the Joint Staff with the responsibility of determining the appropriate response following a cyber attack. Senior military officers were defined as Army, Navy, Air Force, and Marine Corps officers in pay grades O5 (Lieutenant Colonels or Commanders) and above. Cyber divisions were defined as Joint Staff divisions in which the main portfolio focuses on strategic and operational cyber warfare decisions associated with policies, plans, and procedures within the following directorates: J2 (Intelligence), J3 (Operations), J5 (Strategic Plans and Policy), J6 (Computers and Communications), J7 (Operational Plans and Doctrine), J8 (Force Structure and Resources), and Joint Staff Legal. From the total population of nearly 1,500 officers who were serving for the CJCS, approximately 30 senior military officers had the requisite cyber warfighting decision-making experience to be considered the target population for this study.

Sampling Frame

A purposeful (i.e., nonprobability), criterion-based sampling method was used for this phenomenological study (Creswell, 2005; Marshall, 1996a; Mertens, 2005). According to Marshall (1996b), criterion-based sampling is the most effective method for selecting key informants when conducting qualitative research using interviews with experts. Although sample sizes for qualitative studies are small relative to quantitative research, Marshall (1996a) asserted, "An appropriate sample size for a qualitative study is

one that adequately answers the research question” (p. 523). Consequently, the number of required participants, according to Marshall, becomes evident as “the study progresses, as new categories, themes or explanations stop emerging from the data (data saturation)” (p. 523). Therefore, a responsive design is required for qualitative research studies, which incorporate a flexible and iterative approach to (a) participant sampling, (b) data collection and analysis, and (c) results interpretation.

Probability sampling techniques are not appropriate for qualitative research because the sample size is not known a priori (Luborsky & Rubenstein, 1995). Additionally, the required number of participants is not necessarily proportional to the target population. Luborsky and Rubenstein (1995) proposed three considerations when developing the sample selection scheme for qualitative studies. First, the researcher should define the characteristics that represent the system or sample “universe” being studied. Second, the researcher should *sample for meaning* with “the goal of understanding the individuals’ naturalistic perceptions of self, society, and their environment” (Luborsky & Rubenstein, 1995, p. 98). Third, the researcher should select the appropriate nonprobability sampling technique (e.g., convenience, purposeful, snowballing, quota, and case study) that best fits the research design.

A purposeful and homogeneous sampling technique was used in this research study in which participants were deliberately and judiciously selected to represent several explicitly predefined traits, conditions, or criteria (Groenewald, 2004; Luborsky & Rubenstein, 1995; Marshall, 1996a, Polkinghorne, 2005). From the total population of approximately 1,500 officers who serve on the Joint Staff, three criteria distinguished the purposeful and homogenous sample of experts (key informants). The criteria were (a)

senior military officers, (b) work within cyber warfare divisions, and (c) assigned to Joint Staff directorate codes J2, J3, J5, J6, J7, J8, and Legal. An initial review of the total population estimated this criterion-based process would yield at least 30 senior officers with extensive cyber warfare experience. From the list of potential senior officers, the participants were prioritized by military seniority (rank), cyber warfare experience, and time on the Joint Staff when determining the desired interview order and developing the interview schedule.

Because statistical methods were not appropriate for determining the necessary sample size for a phenomenological research study, the number of participants to interview could not be computed by variables or analytical formulas (Cooper & Schindler, 2008). However, Luborsky and Rubenstein (1995) found heuristic “rules of thumb” exist based on “traditions within social science research studies of all kinds, commonsense ideas about how many will be enough, and practical concerns about how many people can be interviewed and analyzed in light of financial and personnel resources” (p. 105). Historical averages indicate 12 to 26 people were necessary to achieve theoretical data saturation for qualitative research studies (Luborsky & Rubenstein, 1995). Therefore, approximately 20 participants were estimated for this phenomenological research study. Accordingly, the number of senior military officers on the Joint Staff meeting the purposeful sampling criteria and available to participate in this research study was sufficient to achieve theoretical data saturation.

Informed Consent

Informed consent was used to ensure research participants understood their rights and the expected level of participation during the interview process. Ethical behavior and

practices, according to Neuman (2005), are essential for social research. Therefore, each senior military officer's participation was voluntary with a thorough understanding of the purpose and scope of the research study (Warren, 2001). Prior to conducting an interview, each participant was provided a full disclosure letter (see Appendix E) describing the research study's purpose and the measures in place to maintain anonymity and confidentiality. Prior to conducting the interview, each participant provided informed consent by reading and signing a formal statement (see Appendix F) that described the interview process and the potential risks and benefits from participating. Authorization and permission to conduct interviews with senior military officers on the Joint Staff within the Pentagon was granted on the signed Joint Staff interview permission form (see Appendix G).

Building on Neuman's (2003) recommendations for constructing an informative consent mechanism that is reassuring and not coercive in any manner, the informed consent form (see Appendix F) was designed to provide the option to participate or withdraw from participation at any time without consequences. Furthermore, the intended data security measures and retention requirements were stressed because the interviews were digitally recorded and transcribed for accuracy and completeness. Because the interviews are with military officers with knowledge and access to sensitive and classified material, each participant was informed that all questions and answers must be unclassified, releasable, and publishable. Last, participants were notified that their individual perceptions and experiences do not reflect the official position of their respective Military Departments, the Joint Staff, the DoD, or the U.S. government.

Confidentiality

In conjunction with establishing informed consent were the processes necessary to protect the privacy, anonymity, and confidentiality of interview participants (Neuman, 2005). Because phenomenological research is intended to interpret the private thoughts, perceptions, and lived experiences of participants, demonstratively establishing precautions to protect the privacy of participants was essential to building trust during the interview process. According to Neuman (2005), researchers protect privacy by separating the respondents' identities from their responses. Researchers accomplish this separation by employing anonymity and confidentiality measures. Anonymity measures refer to the steps required to decouple the participants' names from the respective interview data to protect their identities. Confidentiality measures are the security processes that prevent the names of the respondents from becoming public knowledge in order to protect the participants from physical or emotional harm based on their responses.

For this research study, each participant remained anonymous throughout the data collection process. To achieve participant anonymity, a unique alphanumeric code was individually assigned to each participant's interview data. Each participant provided informed consent by signing the form provided in Appendix F. The signed consent forms and associated interview data will not be related or stored together in any manner. Even though absolute anonymity is not possible for this research design, strict security processes were followed to prevent comingling the signed consent forms with the demographic questionnaires, audio files, or other data collection materials.

Neuman (2005) said, “Confidentiality is a crucial issue and should be guaranteed” (p. 291). To ensure confidentiality, all physical notes, demographic questionnaires, digital recordings, and transcriptions were physically locked and stored in a secure container with controlled access. Digital interview data, including audio and transcription data, were encrypted, password protected, stored on read-only CD-ROMs (one per participant), and labeled using the respective alphanumeric identification code. All research materials and interview data will remain safely stored for a minimum of three years. At the end of the three years, all paper and electronic documents, including the CD-ROMs, will be destroyed, deleted, or shredded. The full disclosure letter (see Appendix E) and the consent form (see Appendix F) contain a summary of the anonymity and confidentiality measures described above.

Geographic Location

The geographic location of this research study was Washington, DC. Senior military officers who make cyber warfare decisions and who serve on the Joint Staff within the Pentagon comprised the population for this study. Because phenomenological research depends on extracting the perceptions from the participants based on their lived experiences, Cooper and Schindler (2008) highlighted the importance of conducting research interviews in the participant’s natural setting if feasible. Cooper and Schindler found perceptual awareness during the interview process more closely resembles the participant’s day-to-day reality when the interview is conducted under actual environmental conditions. Therefore, the interviews were performed in the participant’s normal surroundings and operational spaces within the Pentagon to the maximum extent

possible. Due to scheduling constraints, some interviews were conducted after working hours at locations requested by the participants.

Data Collection

Given the subjective nature of qualitative research, meticulous and rigorous data collection methods are required to improve the validity of the results (Easton, McComish, & Greenberg, 2000). The primary method for collecting data for this research study was through the transcription of digital, audio recordings of individual interviews with the participants. When conducting a qualitative study, Creswell (2005) recommended researchers develop a comprehensive and flexible data collection plan. The plan should have enough detail to answer the questions *who*, *what*, *where*, *when*, and *how* in order to facilitate and improve the effectiveness of the interview process (Cooper & Schindler, 2008). Furthermore, the data collection plan should identify the “observational targets, sampling strategy, and acts (operationalized as a checklist or coding scheme)” (Cooper & Schindler, 2008, p. 206).

Once the participants are identified using the purposeful, criterion-based sampling method described earlier, Creswell (2005) suggested the researcher should determine the type of interview to conduct. When capturing data for a phenomenological research study, individual interviews are the most useful and effective data collection method (Groenewald, 2004; Kvale, 1996; Moustakas, 1994; Priest, 2002). Kvale (1996) asserted the qualitative interview “is literally an *inter-view*, an interchange of views between two persons conversing about a theme of mutual interest,” in which the researcher attempts to “understand the world from the subjects’ point of view, to unfold meaning of [their] experiences” (pp. 1-2). For this research study, personal one-on-one interviews were the

preferred data collection method with telephonic interviews serving as a backup method. The interviews lasted for approximately one hour on average.

Prior to an interview, the qualified participants were sent an electronic copy of the full disclosure letter (see Appendix E), the informed consent form (see Appendix F), the Joint Staff interview permission form (see Appendix G), and the demographic questionnaire (see Appendix H, page 1 of 2). The participants were contacted to establish an interview time and place that accommodated their work schedule and desired interview location. Phenomenological research is enhanced if the interviews can occur within a participant's natural setting or environment where the phenomenon is experienced (Groenewald, 2004; Moustakas, 1994; van Kaam, 1972). Furthermore, the interview location should be a quiet, suitable, and conducive place for conducting and audiotaping the interview that is free from background noise, distractions, and interruptions (Creswell, 2005; Groenewald, 2004). The interviews were held within the participants' offices inside the Pentagon.

Before starting an interview, informed consent was obtained by ensuring the participant read and signed the informed consent form (see Appendix F). Once all questions and concerns about the interview process were answered or addressed, the interview began. A digital, audio recording device compatible with transcription software was used during the interview. The audio recording device was capable of taping telephone interviews as well. According to Creswell (2005), audiotaping the interview is essential for providing an accurate record of the conversation in order to obtain a verbatim transcription. An alphanumeric coding system was employed to protect the participant's anonymity and ensure the confidentiality of the interview data.

An individual code containing the interview date and interview number was used to correlate the consent form, field notes, demographic questionnaire, interview materials, and digital audiotape file.

When conducting a phenomenological research study, in-depth, person-to-person interviews are the most essential element of the data collection process (Donalek, 2004; Groenewald, 2004; Moustakas, 1994). According to Creswell (2007), a phenomenological study requires “long interviews with up to 10 people” (p. 65) to achieve thematic saturation. Boyd (2001) corroborated Creswell’s assertion by considering “2 to 10 participants or research subjects sufficient to reach saturation” (p. 101). Luborsky and Rubenstein (1995) found an average of 12 to 26 people is necessary to achieve theoretical data saturation for qualitative research studies. However, Groenewald (2004) determined “data-collection interviews should continue until the topic is exhausted or saturated, that is when interviewees (subjects or informants) introduced no new perspectives on the topic” (pp. 46-47). During the data collection phase, this research study followed Groenewald’s recommended interview guidance with the expectation that approximately 20 interviews were necessary to reach thematic saturation.

The research study interviews were designed to gain an understanding of the lived experiences and perspectives of senior military officers on the Joint Staff regarding the decision-making uncertainty associated with determining the appropriate response following a substantial cyber attack. Therefore, the data collection process during the interviews supported answering the study’s research question. When conducting the

interviews, Moustakas (1994) proposed several techniques intended to improve the quality and validity of the data gathered.

First, Moustakas (1994) recommended researchers “engage in the epoché process as a way of creating an atmosphere and rapport for conducting the interview . . . by setting aside prejudgments . . . with an unbiased, receptive presence” (pp. 180-181).

Second, the researcher should *bracket* the research question. Bracketing is an essential element of the transcendental phenomenological reduction process where “the focus of the research is placed in brackets [and] everything else is set aside so that the entire research process is rooted solely on the topic and question” (Moustakas, 1994, p. 97).

While performing semi-structured interviews, Moustakas (1994) found the researcher should consider informal, topical-guided interviewing techniques using open-ended questions in order to obtain the most comprehensive and detailed description of the experience. Creswell (2005) added the researcher should use *probes* (or sub-questions) to gain additional insights, elicit more information, and expound on key ideas. Probes can range from “exploring the content in more depth (elaborating) to asking the interviewee to explain the answer in more detail (clarifying)” (Creswell, 2005, p. 218). To support the research question, probes were used to stimulate the participant’s thoughts in order to extract additional experiences and perceptions. The probing questions are listed on the interview form following the lead research question (see Appendix H).

Although the participants were given the opportunity to share their perspectives and thoughts freely and openly, neutral prompts were necessary to maintain the conversational flow as a means of encouraging the emergence of additional thoughts and experiences (Moustakas, 1994; van Manen, 1990). Examples of neutral prompts included

“Please tell me more,” “Describe what you mean by that,” “How did you feel about that?” and “Can you give me an example?” According to Moustakas (1994), prompts for additional information may be required when the interviewer believes in-depth perceptions have not fully emerged based on the in-situ analysis of the participant’s response and body language. When necessary, broad open-ended queries were used spontaneously during the interview for obtaining clarification or more fully developing a particular response.

According to van Manen (1990), the interviewer must be an active listener and intently engaged in order to elicit non-emerged perceptions regarding areas associated with the phenomenon that require further focus. Based on the review of the literature and in support of the theoretical framework, the following list represented broad areas of non-emerged perceptions in which neutral prompting was used:

1. Policy and legal (domestic and international) aspects;
2. Organizational command and control considerations;
3. Rules of warfare concerns;
4. Technological capabilities and attribution challenges;
5. Ethical, cultural, social, and cognitive issues; and
6. Second and third order effects.

Moustakas (1994) found that the adept and timely use of prompts and open-ended queries enhance obtaining the full disclosure of the participant’s experience. The advantage of the phenomenological interviewing method is the ability for the researcher to remain flexible and responsive to the individual direction a particular interview takes without

presuppositions or predetermined outcomes about the phenomenon (Berg, 2004; Patton, 2002).

In addition, Creswell (2005) recommended the researcher take notes during the interviews to capture clarifying thoughts, key concepts, and rationales for follow-up questions or prompts associated with the respondent's answers and if the digital recorder fails. Because taking notes during the interview while asking questions and actively listening is challenging, the notes should be brief and not distracting to the interview process. For each interview, field notes were taken on the interview form (see Appendix H). As the interviews were completed, the digital audio recordings were downloaded and securely stored on a computer. A professional service was used to transcribe the content. The audio recordings were listened to while reading the transcript to ensure the transcription service created an accurate and verbatim written copy. The transcribed interviews were stored both in a printed format and in a computer file for later review and analysis using the QSR NVivo 8 qualitative research software program.

Instrumentation

In comparison to quantitative research in which the creditability depends on instrument construction, Patton (2002) asserted, "The researcher is the instrument" (p. 14) in qualitative research. Therefore, qualitative research, according to Patton, relies heavily on the "skill, competence, and rigor of the person doing the fieldwork" (p. 14). To support the objectives of this research, the main instrument in this phenomenological study were in-depth, semi-structured personal interviews. The phenomenological interview is a dialogue between two individuals in a social, relaxed, and trusting atmosphere (Moustakas, 1994). Interviews are used extensively in qualitative research

because they are the most effective instrument for extracting individual experiences and behavior (Roberts et al., 2003).

Cooper and Schindler (2008) explained the main advantage of the interview process is the researcher's ability and opportunity to respond adaptively to the participant's answers. By skillfully doing so, the researcher can elicit more information and clarify vague statements by building trust and rapport with the participants (Cooper & Schindler, 2008). Therefore, a well-conducted interview obtains information that other data collection methods would likely not reveal.

Roberts et al. (2003) found semi-structured interviews best facilitate the research goal of eliciting the "rich data . . . [associated with] the informant's experiences, feelings, views, or described truth" (p. 231). According to Neuman (2005), face-to-face interviews are preferred because the researcher can observe the surroundings and nonverbal communication cues and visual aids. However, if face-to-face interviews are not possible, Neumann found telephone interviews are just as effective if the researcher continues to explore complex responses with extensive probes using the proper tone of voice and carefully selected question wording. Telephone interviews were not required for the current study.

A questionnaire (see Appendix H) was developed to facilitate and help guide the interview process. The first 10 questions were used to obtain demographic information and assess military experience. In support of the research question, open-ended questions were used to explore and probe for additional information by stimulating recessed memories of related experiences (Moustakas, 1994). Using a semi-structured interview

format, the supporting questions were designed to establish an environment where participants considered the interview as a free-flowing conversation.

According to Burnard (2005), the semi-structured interview format includes a set of questions that contains key areas to be covered, which anticipate potential responses while allowing unexpected responses. Semi-structured interviews permit asking the participants the same set of questions within a flexible framework without a defined ordering of the questions (Dearnley, 2005). In this interview environment, Dearnley (2005) determined, “Participants are encouraged to talk about their experiences through open-ended questions, and the ordering of further questions is determined by their responses” (p. 22).

To support the primary research question, six broad open-ended questions (see Appendix H) were developed as a general interview guide to “facilitate the obtaining of rich, vital, substantive descriptions of the . . . [participant’s] experience of the phenomenon” (Moustakas, 1994, p. 116). In addition, using the study’s theoretical framework and the review of literature as a topical guide, potential non-emerged perceptions may require neutral prompting when the participant’s “story has not tapped into the experience . . . with sufficient meaning and depth” (Moustakas, 1994, p. 116). According to van Manen (1990), the purpose of the interview is to arrive at the essence of the research question. To do so, van Manen asserted researchers must interrogate from the heart of their existence and from the center of their being. A phenomenological question, according to van Manen, “. . . must not only be made clear, understood, but also ‘lived’ by the researcher” (p. 44).

Validity and Reliability

Reliability and validity are fundamental measurement characteristics for all research methods (Neuman, 2005). Quality research is dependent on the source data and measurement processes being both reliable and valid. Reliability, according to Neuman (2005), implies the measurements are dependable and repeatability consistent. Neuman further defined validity as “truthfulness . . . or the way the researcher conceptualizes the idea in a conceptual definition, and a measure” (p. 179). Whereas reliability is a measure of confidence that the same results would be achieved if the study were to be replicated, validity is a measure of the researcher’s ability to draw meaningful and justifiable inferences about the population (Berg, 2004; Creswell, 2005). According to Priest (2002), researchers must exercise rigor to ensure “qualitative research, including phenomenological approaches . . . is believable, accurate, and right, and useful to people beyond those who participated in it” (p. 57). To demonstrate this rigor, researchers must duly consider the means to achieve validity, reliability, and generalizability when conducting research studies (Priest, 2002).

Validity. For this research study, internal validity (i.e., the ability for the research instrument to function as designed) and external validity (i.e., the ability to generalize causal relationships to other populations or situations) were considered. Cooper and Schindler (2008) determined, “Internal validity occurs when the conclusion(s) drawn about a demonstrated experimental relationship truly implies cause” (p. 705). External validity, or generalizability, is the “extent to which findings are transferable to, or fitting for, other situations” (Priest, 2002, p. 60). The concept of validity has traditional linkage to the positivist paradigm as “the result and culmination of empirical conceptions [such as] universal laws, evidence, objectivity, truth, actuality, deduction, reason, fact, and

mathematical data” (Golafshani, 2003, p. 599). Consequently, Golafshani (2003) discovered that some qualitative researchers argue that the concept of validity does not apply to qualitative studies. However, Creswell (2005) asserted that all research methods, including those used in qualitative studies, require a qualifying process or measure.

For qualitative research studies, internal validity is the result of rigorously applying processes that improve quality, trustworthiness, and defensibility of research data (Golafshani, 2003; Hycner, 1985; Neuman, 2005; Priest, 2002; van Kaam, 1959). Therefore, rigor is an essential element for improving validity when conducting qualitative research. Priest (2002) suggested several methods for achieving rigor while increasing [internal] validity including:

1. Making explicit presuppositions and acknowledging subjective judgments;
2. Prolonged engagement with the data;
3. Verification with the source/participant feedback; using low inference descriptors, such as extracts from participant’s verbatim account; and
4. Peer debriefing, whereby ongoing analysis and findings are regularly presented to others for peer evaluation. (pp. 59-60)

By establishing internal validity, the researcher is able to extract defensible conclusions regarding textual and structural relationships based on the data (Priest, 2002). Therefore, quality research studies depend on discovering the truth through measures of building trust (Golafshani, 2003) and instilling confidence in the resultant findings (Lincoln & Guba, 1985).

Another important method of ensuring the internal validity of qualitative research data is through *triangulation* (Denzin, 1978; Farmer, Robinson, Elliott, & Eyles, 2006; Leech & Onwuegbuzie, 2007). Farmer et al. (2006) defined triangulation as “a methodological approach that contributes to the validity of research results when multiple methods, sources, theories, and/or investigators are employed” (p. 377). Jick (1979) suggested, “Triangulation may be used not only to examine the same phenomenon from multiple perspectives but also to enrich our understanding by allowing for new or deeper dimensions to emerge” (pp. 603-604). In Denzin’s (1978) germinal work, four triangulation techniques were identified: (a) methodological triangulation, (b) data triangulation, (c) theoretical triangulation, and (d) investigator triangulation.

For the current study, data triangulation was the primary approach used. Data triangulation was used to validate the research findings through multiple data sources including interview transcriptions, field notes, and expert panel feedback (Farmer et al., 2006). Denzin (1978) termed this triangulation approach “within-method” when multiple techniques are used to collect and interpret the data *within* a single research method. Conducting textual analyses of external reports, documents, and studies is an accepted triangulation method to validate qualitative research findings. However, the literature gaps and limitations that were described in chapter 2 prevented this method from being employed (Farmer et al., 2006; Jonsen & Jehn, 2009; Leech & Onwuegbuzie, 2007).

External validity is related to the generalizability of a research study’s results. Neuman (2005) explained that strong external validity permits the extension or generalization of the results to many other scenarios, events, or groups. In contrast, weak external validity implies the results are only applicable to the actual sample or setting that

was researched. Because the goal of qualitative research is to study a specific group, circumstance, or setting, generalizability is considered a weak point in phenomenology (Creswell, 2005; Priest, 2002).

Hycner (1985) stressed that the phenomenological researcher's goal is to describe human phenomena and not, in the purest sense, generalize the findings. However, Golafshani (2003) suggested maximizing the credibility, defensibility, and trustworthiness of the study results may lead to generalizability. Furthermore, in order to determine the extent to which the findings may be generalized, Priest (2002) recommended the qualitative researcher provide the reader comprehensive information associated with the participants' demographics, sampling and selection methods, the interview context, and the data generation and analysis processes.

Reliability. Reliability is the result of conducting quality research with processes that are dependable and consistent (Neuman, 2005). By achieving reliability, confidence is gained that the same results would occur if the study were repeated under identical or very similar conditions (Neuman, 2005). Because specific, purposeful samples are used generally with phenomenological studies, repeatability is challenging because the research is conducted under unique conditions, settings, and social circumstances. Lincoln and Guba (1985) stated, "Since there can be no validity without reliability, a demonstration of the former [validity] is sufficient to establish the latter [reliability]" (p. 316). Priest (2002) found the following methods improve the reliability of the data generation procedures:

1. Providing evidence of an audit trail;
2. Disclosing personal orientation and context;

3. Having intensive engagement with the material and iteration between data and interpretation;
4. Grounding interpretations within the data through the use of verbatim illustration; and
5. Ensuring technical accuracy in recording and transcribing. (p. 60)

Last, Golafshani (2003) determined that consistency is achieved when the research procedures are verified through a rigorous and repetitive assessment of the source data, analysis products, and reduction process notes.

Expert panel review. According to Langfeldt (2004), expert review is “generally seen as the only legitimate method for valuing research quality” (p. 52). An expert panel is a small group of knowledgeable and skilled practitioners within the particular field under study used to evaluate, assess, and validate the population sampling criteria, research questions, and data collection instrument (Beecham, Hall, Britton, Cottee, & Rainer, 2005). Ramirez (2002) submitted that subject matter experts (SMEs) have a “broad, unique insight on target populations and the information requested by a study . . . but who are not prospective respondents” (p. 1). Further, SMEs are effective at assessing and providing feedback regarding the “respondent knowledge, motivation, and authority to respond, levels of sensitivity or threat, burden, respondent selection criteria” (Ramirez, 2002, p. 1).

For the current study, two expert reviews were conducted. First, in accordance with Joint Staff policy, the Joint Staff Historian reviewed and approved conducting this research study (see Appendix G). This review was necessary to ensure the study’s security measures and protocols were adequate to prevent the collection or dissemination

of any classified, sensitive, or “for official use only” content. Second, the study was given to three cyber warfare experts serving for the Information and Cyberspace Policy Directorate for the purpose of conducting a technical review and providing feedback.

With a contextual understanding of the research study’s problem and purpose statements in addition to the research question and associated questionnaire (see Appendix H), the expert panel evaluated the proposal for accuracy, relevancy, difficulty, and content validity. Recommended changes were consolidated, evaluated, and incorporated, as appropriate, into the study prior to conducting the interviews. A similar process was conducted on the textural and structural descriptions, findings, and conclusions to ensure the research study was free of any potentially classified or sensitive material (see Appendix P). Further, the expert panel was used to validate the findings in support of data triangulation.

Pilot study considerations. Pilot studies are inappropriate for qualitative research methods (Holloway, 1997; Morse, 1997; Robson, 2002). Unlike quantitative studies in which the theoretical structure is well developed and established at the proposal stage, Morse (1997) asserted, “The difficulty in qualitative inquiry is that, until the data are saturated, the theoretical scheme is not developed, and in pilot studies, by definition, data are not saturated” (p. 323). Morse further argued that applying the rationales for conducting a pilot study that normally hold for quantitative designs are illogical for qualitative designs. Because a primary reason for conducting qualitative research is that little is known about the topic, conducting a pilot study, in which the data set is small, would be inherently “inaccurate, misleading or incomplete . . . and would not serve as a

very useful indicator of trends to be found in the subsequent larger study” (Morse, 1997, p. 323).

Although pilot studies are essential in quantitative research, in qualitative approaches pilot studies are not necessary because the researcher has the flexibility to “learn on the job” (Robson, 1993, p. 185). Additionally, for qualitative studies, the small number of participants makes pilot studies difficult because there may not be enough informants who fulfill the criteria required by the purposeful sampling process (Holloway, 1997). Furthermore, because qualitative studies typically rely on pattern recognition, Morse (1997) noted, “If data are thin, these patterns are much more difficult to discern, categories are not formed, and themes may not appear” (pp. 323-324). Because pilot data are not saturated, the large variability and likely inconsistency made a pilot study inappropriate for this qualitative research study.

Data Analysis

Priest (2002) depicted Husserl’s (1931) phenomenological method with four fundamental processes: “intentionality; phenomenological reduction; description; and essence” (p. 51). Intentionality is the process of focusing the mind on a specific object or idea (Priest, 2002). Phenomenological reduction enables the transcendence of a conscious thought to a natural attitude using bracketing, eidetic reduction, epoché, and imaginative variation (Bednall, 2006; Giorgi, 1985; Groenewald, 2004; Priest, 2002). Once reduction is accomplished, the researcher can begin describing the central phenomenon in order to determine its essential structure (Castro, 2003; Dowling, 2007; Priest, 2002). With these general processes in mind, Priest found most phenomenological data analysis follow a systematic and prescribed set of steps, including “the division of

text into units; the transformation of units into meanings expressed as phenomenological concepts; and the tying together of transformed meanings into a general description of the experience” (p. 55).

Donalek (2004) suggested, “Research is not truly phenomenological unless the researcher’s beliefs are incorporated into the data analysis” (p. 516). Generally, the phenomenological research process is comprised of formulating study questions, creating an interview guide, selecting key informants, conducting interviews, taking adequate notes, analyzing interview data, checking for reliability and validity, and presenting the findings (Binnendijk, 1996; Castro, 2003; Moustakas, 1994). Therefore, data analysis is an essential element of phenomenological research (Castro, 2003). Of the various methods of conducting phenomenological data analysis, Castro (2003) noted van Kaam (1966), Colaizzi (1978), and Giorgi (1985) constructed the three most widely accepted methodologies. Similar for each method, Dowling (2007) found, “The original descriptions are divided into units, the units are transformed by the researcher into meanings that are expressed in psychological and phenomenological concepts, and the transformations are combined to create a general description of the experience” (p. 135).

Understanding the differences between the various data analysis methods associated with transcendental phenomenology is vital to conducting valid qualitative research. In order to describe human experience as conscious awareness, van Kaam (1959) developed the “psycho-phenomenological method” of describing and analyzing qualitative data as a four-stage (analysis, translation, transposition, and phenomenological reflection), 12-step process (Anderson & Eppard, 1998). Colaizzi’s (1978) method yields a rich interpretation of the fundamental structure of the phenomenon using Husserlian

descriptive principles vis-à-vis a seven-step process that builds on understanding the respondent's transcript as a whole. Giorgi's (1985) method of *imaginative variation* captures the "transcendence from natural to phenomenological attitude . . . [which] involves asking questions of the phenomenon in order to remove inessential features and to test its limits, and exploring all possible meanings of the data" (p. 52).

Selecting the most appropriate phenomenological data analysis method requires an evaluation of the various methodologies based on the type of research that best fits the study's goals and objectives (Priest, 2002). For the current study, the methods of van Kaam (1966), Keen (1975), Colaizzi (1978), Tesch (1980), and Giorgi (1985) were evaluated using criteria established by Hycner (1985), Moustakas (1994), and Priest (2002). Based on this assessment, van Kaam's psycho-phenomenological method as modified by Moustakas was considered the most suitable, methodical, and meticulous process of revealing and analyzing qualitative data (Anderson & Eppard, 1998). The modified van Kaam method is an appropriate research design to accomplish the study's goals because the methodology incorporates a systematic approach for organizing, analyzing, and synthesizing the data (Moustakas, 1994). Furthermore, when deriving data from human science research using "first-person reports of life experiences" (Moustakas, 1994, p. 84), the use of the modified van Kaam method for analysis is preferable.

The modified van Kaam research method is appropriate when the researcher desires to learn from a purposive sample of participants the perceptions, meaningful interpretations, and experiences associated with a central phenomenon under investigation (Moustakas, 1994; Muto & Martin, 2009). The modified van Kaam method

is frequently used for transcendental phenomenological reduction because the “investigator abstains from making suppositions, focuses on a specific topic freshly and naively, constructs a question or problem to guide the study, and derives findings that will provide the basis for further research and reflection” (Moustakas, 1994, p. 47). Understanding the inherent and integral relationship between the researcher and participant, Moustakas asserted the modified van Kaam method provides a rational, consistent, methodical, and reflective process for conducting the phenomenological approach in order to extract and synthesize the essential perceptions and experiences.

To conduct the data analysis process, Moustakas’ (1994) modification to the van Kaam method of analyzing phenomenological data was used to categorize and construct the experiences, perceptions, and perspectives of senior military officers using the following seven-step process:

1. Listing and preliminary grouping (horizontalization);
2. Reduction and elimination to determine the *invariant constituents*;
3. Clustering and thematizing the invariant constituents;
4. Final identification of the invariant constituents and themes (validation);
5. Construction of an individual textural description of experience;
6. Construction of an individual structural description of the experience; and
7. Construction of a textural-structural description of the meanings and essences of the experience. (pp. 120-121)

After applying the above steps, a computer-facilitated process was employed “to access, manage, shape, and analyze detailed textual . . .” (QSR International, 2007, para. 1) and

constructed interview data by categorizing words and phrases into coded behavioral themes using QSR NVivo 8 qualitative research software program.

To obtain a better understanding of the collected data, the digital recording and associated transcription for each interview was repetitively reviewed “to become familiar with the words of the informant in order to develop a holistic sense, the *gestalt*” (Groenewald, 2004, p. 50). According to van Kaam (1959), the term “*gestalt*” (p. 69) captures the idea that the cognitive distinction made between perceptual and emotional events may not be separate in reality because the overall meaning forms during the interaction within a specific interview context. During data analysis, a process called *horizontalization* was used to assemble the primary data into general units of meaning while disregarding material not applicable to the research topic (Moustakas, 1994).

The data analysis process was continued by thoroughly reviewing each participant’s transcribed interview checking the components for uniqueness, overlap, and repetitiveness. By rigorously applying this *thematizing* procedure, redundant components were excluded from further consideration and only properly grouped experiences became part of the core themes. Core themes, according to Moustakas (1994), are the *invariant constituents* that result from the phenomenological reduction and bracketing process in which the descriptive essences of the participant’s narrative, perceptions, and experiences are constructed. The data analysis process was assisted by using QSR NVivo 8 qualitative research software program.

Summary

In chapter 3, a detailed explanation of the qualitative, phenomenological research method used for this study was presented (Creswell, 2005; Donalek, 2004; Groenewald,

2004; Kvale, 1996; Moustakas, 1994; van Kaam, 1959, 1966, 1972). Included in this presentation was a discussion of the research design, population, sampling method, research question, data collection and analysis methods in addition to the means of establishing and maintaining validity and reliability. For the current study, van Kaam's (1959, 1966) phenomenological method as modified by Moustakas was considered the most suitable process of revealing and analyzing qualitative data obtained from interviews that were conducted with a purposeful sample of senior military officers serving on the Joint Staff in Washington, DC (Cooper & Schindler, 2008; Creswell, 2005; Marshall, 1996a, 1996b; Mertens, 2005).

In order to expose relevant perceptions, lived experiences, and key themes, data collected from the field notes and verbatim transcriptions of the digitally recorded interviews were meticulously analyzed using QSR NVivo 8 qualitative research software program. Data triangulation and rigorous checks applied during this process improved the study's validity and reliability (Golafshani, 2003; Priest, 2002). Interviews were conducted until theoretical saturation (i.e., the point where no additional key themes emerge) was reached (Creswell, 2005; Luborsky & Rubenstein, 1995). In chapter 4, the findings from the phenomenological reduction process and analysis of data collected from the face-to-face interviews that were conducted in support of this research study are presented.

Chapter 4: Results

The purpose of this qualitative, phenomenological research study was to explore the decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack. As described in chapter 3, a qualitative method and phenomenological design was used in this study. A qualitative research method is used when exploring a phenomenon such as decision-making uncertainty by inductively analyzing the rich data collected in the participants' natural setting (Bryman, 1984; Bryman et al., 1988; Conger, 1998; Creswell, 2007; Leedy & Ormrod, 2010; Neuman, 2005; Yukl, 1989). A phenomenological design is used to gain an understanding of the essence and meaning of the central phenomenon from the viewpoints, insights, subjective perceptions, and lived experiences of the research participants (Giorgi, 2006; Moustakas, 1994; van Manen, 1990).

Chapter 4 includes a comprehensive analysis of face-to-face interviews with 21 senior military officers who served for the CJCS in Washington, DC. The analysis was based on van Kaam's (1959, 1966) phenomenological reduction process as modified by Moustakas (1994). Prior to the interview process, an expert panel comprised of three select Joint Staff cyber warfare officers validated the research study with emphasis on the research design, purposeful sampling criteria, and interview questionnaire. In-depth personal interviews were conducted until information addressing the central research question reached saturation and no additional themes emerged. The audio-recorded interviews were transcribed and analyzed using QSR NVivo 8 software, which facilitated organizing and managing the textual data in support of the reduction, elimination, pattern recognition, and thematic clustering processes.

The purpose of chapter 4 is to present the key themes based on the participants' lived experiences that emerged from the data collection and phenomenological analysis procedures. The data collection process consisted of conducting and digitally recording semi-structured interviews with 21 senior military officers. The recorded interviews were precisely transcribed and systematically examined using phenomenological analysis techniques designed to understand the meanings and essences of the participants' perceptions and experiences regarding the central research question (Groenewald, 2004; Kvale, 1996; Moustakas, 1994). The research findings described in chapter 4 include the conclusions of an expert panel review, a statistical description of the sample demographics, an explanation of the data collection and coding procedures, a presentation of the data analysis including the thematic portrayal and synthesis of invariant constituents and key themes, and a summary of the results.

Expert Panel Review

Prior to conducting the data collection interviews, an expert panel was used to assess the understandability of the central research question from a cyber warfare perspective and confirm the validity of the research objectives and protocol. Expert judgments "lend objectivity, credibility, and rigor to the review and assessment of a research study" (Oros, Doan, Adoum, & MacDonald, 2007, p. 157). Yin (2009) asserted that using an expert panel within the given discipline area is an excellent method for validating the data collection instrument and clarifying the research question formatting and meaning. To assess the quality of research, Langfeldt (2004) submitted that each panel member should "... be a 'peer' of the researcher under review [and] an expert in the area" (p. 52). Therefore, the expert panel was assembled with SMEs who met the

same professional standards as the purposeful sampling criteria used for the data collection interviews.

The expert panel was comprised of three select Joint Staff officers serving for the Information and Cyberspace Policy Division of the J5 Directorate. The expert panel was used to evaluate the study's research question, interview process, and purposeful sampling criteria. The panel was requested to assess the effectiveness of the research design with respect to achieving the study's objectives from the perspective of a senior cyber warfare officer. The three expert reviewers included one Navy Captain, one Air Force Colonel, and one Marine Colonel. Each SME had over 20 years of active duty military service and over one year making cyber warfare decisions at the national level on the Joint Staff. Each reviewer received a briefing on the purpose of the research study and signed the same informed consent form (see Appendix F) as the study participants.

The expert panel was provided a copy of the research study proposal to ensure each member had the proper context and background for making informed judgments. Providing this material had the additional value of ensuring the study was free of classified or sensitive material in accordance with Joint Staff policy. The panel was asked specifically to provide candid feedback and constructive criticism regarding the central research question and interview questionnaire (see Appendix H). The SMEs ensured the adequacy of the demographic questions, commented on the clarity of the research question, and offered several recommendations. The feedback from the expert panel was instrumental in developing better techniques for conducting the phenomenological interviews, providing confidence that the research question was clear and understandable, and ensuring the validity and reliability requirements of the research

study were met. The expert panel agreed that the purposeful sampling criteria for selecting the participants for the research study were appropriate.

Sample Demographics

A purposeful, criterion-based sampling method was used for this phenomenological study (Creswell, 2005; Marshall, 1996a; Mertens, 2005). According to Marshall (1996b), criterion-based sampling is the most effective method for selecting experienced and knowledgeable participants within a specific group or particular area of expertise. When a criterion-based selection process is used, a *homogeneous* sample is produced. Polkinghorne (2005) found homogeneous samples should be used when “describing the experience of a particular subgroup in depth” (p. 141). A purposeful and homogeneous sampling technique was used in the current research study in which participants were specifically selected from approximately 1,500 officers who served on the Joint Staff (Groenewald, 2004; Luborsky & Rubenstein, 1995; Marshall, 1996a; Polkinghorne, 2005). Three explicitly defined criteria based on military rank, military Service, and cyber warfare experience was used during sample selection process.

The sample consisted of 21 senior military officers assigned to the Joint Staff. Each participant was over the age of 18 and volunteered to be interviewed. The purposeful selection process was designed and executed to ensure the sample accurately represented the Joint Staff cyber warfare leadership population. This included identifying senior military officers of varying ranks between pay grades O5 to O7 from all four military Services currently serving in a Joint Staff cyber warfare division. The sample included cyber warfare experts whose roles and responsibilities included operational, strategic policy, computer network, doctrinal, organizational, and legal experience. The

participants, as co-researchers, were urged to share and describe their perspectives and lived experiences openly and honestly. Further, the participants were assured that all interview information would remain confidential and that their identity would be kept anonymous by following stringent data collection, storage, and coding procedures.

Demographic information was collected to document the participants' ages, genders, military ranks, education levels, branches of Service, years of military and cyber warfare experience, and level of formal cyber warfare training. The demographic information category selections supported the purposeful sampling criteria and the research analysis of the interview content. Participants' ages ranged from 34 to 53 with an average age of 43. The age distribution is shown in Table 1. The sample included 15 men and 6 women. The 15 male participants represented 71% of the study population. This corresponded well with the actual gender demographics serving within cyber warfare divisions on the Joint Staff in which 77% are male (D. A. Hoopes, personal communication, June 14, 2010).

Priest (2002) noted that Husserl believed that "access to the material world was through consciousness, and that all knowledge was derived from *experience*" (p. 51). Therefore, understanding and describing experience is the essence of a phenomenological research study (Hycner, 1985; Moustakas, 1994; van Kaam, 1959). Accordingly, key demographics that reflect the level of experience of the participants are essential to the external validity of this research study (Golafshani, 2003). A review of the literature indicated that measures of experience are important factors for understanding decision-making and leadership phenomena (Bryman et al., 1988; Hertwig, Barron, Weber, & Erev, 2004; Schultz, 1997). Therefore, specific demographic factors for military

experience should include age, pay grade, roles, responsibilities, education, time in position, and years of service (Avery, Tonidandel, Griffith, & Quiñones, 2003; Bryant & Wilhite, 1990; Campbell & McCormack, 1957; Schell, Youngblood, & Farrington, 2008).

Table 1

Participants' Age Distribution

Age Groups	Participants	
	n	%
34-39	5	24
40-44	5	24
45-49	7	33
50-53	4	19
Total	21	100

Interviews were conducted with 21 senior military officers in paygrades O5, O6, and O7 as shown in Table 2. When the interviews were conducted, the actual paygrade distribution within Joint Staff cyber warfare divisions was O5 (56%), O6 (30%), and O7 (14%; D. A. Hoopes, personal communication, June 14, 2010). The decision to select and interview proportionally more senior officers for this research study was purposeful and desirable for gaining the most evolved understanding of the central phenomenon. When studying decision-making uncertainty, Dane and Pratt (2007) argued that the most mature and experienced research participants should be used because rational judgment, enlightened perspectives, and effective intuition typically scale with leadership position and organizational seniority.

Table 2

Participants' Military Rank Distribution

Military Rank (Paygrade)	Participants	
	n	%
O5	10	48
O6	7	33
O7	4	19
Total	21	100

Participants from all four military Services were interviewed (see Table 3). The actual military Service distribution for Joint Staff cyber warfare divisions was Army (12%), Navy (28%), Air Force (48%), and Marines (12%; D. A. Hoopes, personal communication, June 14, 2010). The interviews were conducted to match the actual military Service distribution as closely as possible to enhance the validity of the study. When the research sample accurately reflects the population, the research findings are more trustworthy, credible, and defensible because data collection quality and bias are better controlled (Golafshani, 2003).

Gaining the perspectives of senior officers from each military Service is inherently important when conducting a research study involving the Joint Staff. According to Roman and Tarr (1998), the purpose of the JCS is to “rise above any particular Service interest to address the nation’s security interests by contributing a unified perspective” (p. 92). The Joint Staff facilitates inter-Service coordination by precluding unique Service *personalities* (parochially developed over time by distinctive

ideological and doctrinal orientations) from dominating vital decision-making processes or interagency policy (Roman & Tarr, 1998).

Table 3

Participants' Military Service Branches

Military Service	Participants	
	n	%
Army	3	14
Navy	6	29
Air Force	9	43
Marines	3	14
Total	21	100

Interviews were conducted with senior military officers serving on the Joint Staff in cyber warfare divisions as described in Table 4. The interviews were closely aligned to the actual distribution of officers serving within cyber warfare divisions, which was J3 (25%), J5 (47%), J6 (12%), J8 (4%), and Legal (8%; D. A. Hoopes, personal communication, June 14, 2010). No interviews were conducted with officers from the J2 (Intelligence), J4 (Logistics), or J7 (Doctrine) Joint Staff directorates for this research study. This purposeful data collection decision was based on feedback from the expert panel. The expert panel recommended that the interviews focus on the Joint Staff directorates that conduct the preponderance of the cyber warfare response decisions. This recommendation is consistent with the guiding principles associated with purposeful, nonprobability, criterion-based sampling methods in which participants that

best represent pre-defined traits or conditions are selected (Creswell, 2007; Luborsky & Rubinstein, 1995).

Table 4

Participants' Joint Staff Directorate Codes

Joint Staff Code (Cyber Warfare Division)	Participants	
	n	%
J3 (Operations)	5	23
J5 (Strategic Policy)	11	52
J6 (Computer Networks)	2	10
J8 (Force Structure)	1	5
Legal (General Counsel)	2	10
Total	21	100

As indicated in Table 5, the research participants' military experience levels ranged from 14 to 31 years with an average of 22 years of service. In addition, each participant had over 1 year of cyber warfare decision-making experience with an average of 2.4 years on the Joint Staff (see Table 6). Experience as measured by time (or tenure) is the most predictive determination of leadership and decision-making effectiveness (Avery et al., 2003). In addition, Avery et al. (2003) asserted that experience in a subordinate's job and experience under high stress conditions substantially add to the validity of traditional tenure measures of leadership efficacy. These measures of experience are particularly important for military officers because they serve as the primary criteria for promotion boards and selection processes to positions of responsibility (Bettin & Kennedy, 1990; Fiedler, 1992).

Table 5

Participants' Years of Military Experience

Years of Military Service	Participants	
	n	%
14-19	8	38
20-25	8	38
26-31	5	24
Total	21	100

The participants' education levels were well above the national averages for postgraduate degrees (based on census data) in which 8.9% hold a Master's degree and 3% hold a professional degree (Stoops, 2004). For this research sample, 100% of the participants held a Master's degree, 52% held two or more Master's degrees, and 14% held a professional degree. Holder and Murray (1998) noted, "Education has historically played a major role in preparing military officers for war . . . by teaching them standard practices, encouraged innovation, and realism in decision-making during the stress and confusion of battle" (p. 81). According to Thirtle (2001), military leaders value education equal with experience, training, and performance. Thirtle also found that professional education improves productivity, retention, and morale. A military officer's formal education level is an important consideration for promotion board selectivity (Thirtle, 2001), duty assignment opportunities (Holder & Murray, 1998), and understanding the consequences of decisions and acts (Micewski, 2003).

Table 6

Participants' Years of Cyber Warfare Experience

Years on Joint Staff (Cyber Warfare Division)	Participants	
	n	%
1 - 2	6	29
2 - 3	12	57
3 - 4	3	14
Total	21	100

Data Collection Process

The data collection process consisted of precisely transcribing digital, audio recordings of personal one-on-one interviews conducted to explore the perceptions and experiences of senior military officers. As the primary instrument of phenomenological research, interviews should be conducted to illuminate meaning within the social context of the experience (Kvale, 1996; Wimpenny & Gass, 2000). During the interviews, meaning emerges as a “co-creation between the researcher and the researched and not just the interpretation of the researcher” (Wimpenny & Gass, 2000, p. 1487). With traditional phenomenology, participants are considered co-researchers versus data repositories (Donalek, 2004; Kvale, 1996; Moustakas, 1994). Therefore, the subjective nature of qualitative research is dependent on the data collection process (i.e., personal interviews and verbatim transcriptions) being conducted carefully to ensure the method is reliable and the results are valid (Creswell, 2007; Easton et al., 2000).

Interview process. Comprehensive and intimate interviews were conducted with 21 senior military officers serving on the Joint Staff. The expert panel approved the list

of participants using the purposeful selection criteria. Prior to an interview, the qualified participants were sent an electronic copy of the full disclosure letter (see Appendix E), the informed consent form (see Appendix F), the Joint Staff interview permission form (see Appendix G), and the demographic questionnaire (see Appendix H, page 1 of 2). Interviews were completed over a four-day period between March 23, 2010 and March 27, 2010. Each interview lasted between 45 and 75 minutes. The interviews were conducted at a mutually agreed upon time and location within the participants' offices inside the Pentagon. Phenomenological interviews are typically more productive when they occur within a participant's natural setting or environment where the phenomenon is experienced (Groenewald, 2004; Moustakas, 1994; van Kaam, 1972).

Before starting an interview, each participant read and signed the informed consent form (see Appendix F). During this period, each participant was afforded many opportunities to ask questions about the research study and to verify their understanding of the interview process including the sample criteria, confidentiality and anonymity procedures, and permission requirements. Each participant was asked to reaffirm his or her permission to be digitally recorded during the interview. When all questions and concerns about the interview process were answered or addressed, time was spent establishing a respectful atmosphere and professional rapport. Once a comfortable and uninhibited environment was developed, participants were asked to express freely and openly their thoughts and perceptions to the following lead interview question:

Please describe the decision-making uncertainty you experience when determining the appropriate response to a cyber attack.

During the semi-structured interviews, a responsive and enticing atmosphere was maintained by using personalized and spontaneous probes and queries to stimulate conversational flow and to encourage the emergence of additional thoughts and experiences. Epoché and bracketing techniques were used to set aside preconceptions and presuppositions about the central phenomenon in order for the participants' perceptions and experiences to be revealed and understood in their purest and most meaningful form (Bednall, 2006; Husserl, 1931; Moustakas, 1994). Neutral prompts and broad open-ended questions, similar to those listed on the interview form (see Appendix H), were used to create a collaborative environment for gaining clarifications and elaborations when necessary to capture the participants' insights and thoughts more fully. When conducting phenomenological research, Moustakas (1994) found that follow-up questions are often inspired and most effectively developed in-situ as the richness of the participants' perceptions and experiences are revealed.

Transcription process. Each interview was recorded with a digital, audio recording device. All interviews were conducted in person versus other communication methods (e.g., telephone, video-teleconference, etc.). Audiotaping the interview provides an accurate record of the conversation in order to obtain a verbatim transcription (Creswell, 2005). The digital files were electronically coded, downloaded to a personal computer, and stored within a password-protected folder. When not in use, the hardcopy files associated with the interviews were stored in a locked file cabinet. During the interviews, field notes were taken on the interview form (see Appendix H) to capture clarifying thoughts, key concepts, and rationales for follow-up questions or prompts associated with the participant's answers. The field notes were also helpful for

understanding the transcribed interviews and used frequently during the data analysis process in order to triangulate the findings.

The digitally stored recordings of the interviews were sent via secure means to a professional, third party transcription service. Confidentiality and anonymity measures were taken by ensuring no personal identification information was part of the audio files. Further, the audio files were labeled with a unique alphanumeric code known only to the researcher. The independent transcription service had a long-standing, reputable record and conducted business with a professional and reliable confidentiality agreement. The transcription service returned the files as Microsoft Word documents. The audio recordings were carefully compared to the associated transcribed document to ensure an accurate and verbatim written copy was produced. The transcribed files were provided to the Joint Staff expert panel for review to ensure the documents were free of classified or sensitive material (see Appendix P). Further, the expert panel was used to validate the findings as a component of the data triangulation strategy.

An individual alphanumeric code containing the interview date and interview number was used to correlate the consent form, field notes, demographic questionnaire, interview materials, digital audiotape files, and transcriptions. The alphanumeric coding system was designed to protect the participant's anonymity and ensure the confidentiality of the interview data. To facilitate the phenomenological reduction process, the audio and transcribed files were imported into QSR NVivo 8 textual analysis software. An individual source case was created for each transcribed file and linked to the respective participant's demographic attributes. The next section describes how phenomenological reduction was used to analyze the experiential narrative data in order to identify common

patterns, invariant constituents, key themes, and textual-structural descriptions (Moustakas, 1994).

Data Analysis and Presentation of Findings

Moustakas' (1994) modification to van Kaam's (1959, 1966) method of phenomenological data analysis was used for this research study. When analyzing narrative data from "first-person reports of life experiences" (Moustakas, 1994, p. 84), the modified van Kaam method is preferable. This method was considered the most appropriate research design after evaluating and comparing the methods of van Kaam, Keen (1975), Colaizzi (1978), Tesch (1980), and Giorgi (1985) using criteria established by Hycner (1985), Moustakas (1994), and Priest (2002). Similar for each method, a reduction process is followed in which narrative descriptions are divided into units of meaning, transformed into phenomenological concepts, and combined to create a composite description of the experience (Dowling, 2007). Once reduction is accomplished, the researcher seeks to determine the essential structure of the central phenomenon (Castro, 2003; Dowling, 2007; Priest, 2002). Therefore, data analysis is a necessary element of phenomenological research (Castro, 2003).

For phenomenological research studies, in-depth, person-to-person interviews are required with approximately 5 to 25 participants to reach theoretical data saturation (Boyd, 2001; Creswell, 2007; Luborsky & Rubenstein, 1995). Groenewald (2004) emphasized that data collection interviews should continue until the informants introduce no new perspectives or describe no additional horizons of the experience. According to Guest, Bunce, and Johnson (2006), reaching theoretical saturation cannot be determined in the field while conducting the interviews because of the detailed, post-facto analysis

required. Therefore, Marshall (1996a) noted that the number of participants available for interviews should be sufficient to ensure “new categories, themes, or explanations stop emerging from the data” (p. 523). For the current study, the data analysis process was used to determine theoretical saturation occurred after 18 interviews. This finding was confirmed by analyzing three additional interviews. Figure 6 illustrates how theoretical data saturation occurred for the current study.

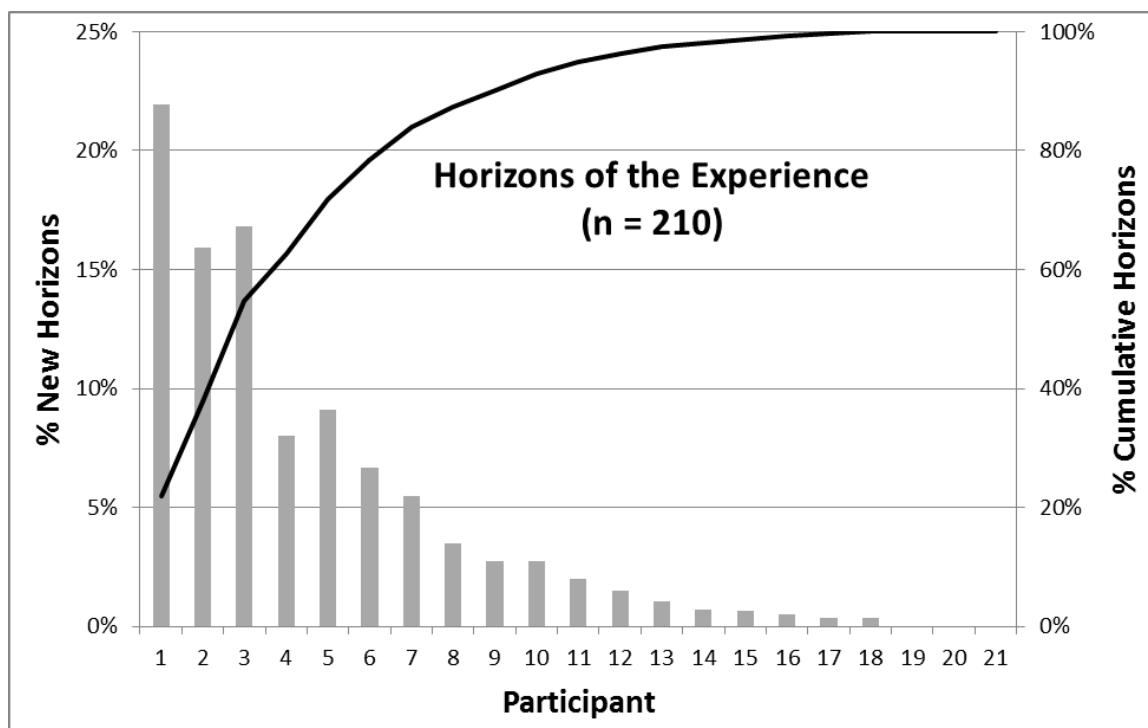


Figure 6. Theoretical saturation of thematic data occurred after 18 interviews as verified during the horizontalization process of the phenomenological reduction analysis.

The modified van Kaam method was used as a systematic approach for organizing, analyzing, and synthesizing the textual data (Moustakas, 1994). The interview audio files, the associated transcriptions, and the field notes were used throughout the data analysis process in order to extract and synthesize the essence of the experiences. Specifically, Moustakas’ (1994) seven-step process was used to analyze,

categorize, and construct the perspectives of the participants using QSR NVivo 8 qualitative research software to manage the coded narrative data and experiential themes. Groenewald (2004) suggested that software should be used to “ease the laborious task of analyzing text-based data through rapid and sophisticated searches and line-by-line coding . . . [however] these programs do not help with the understanding of the meaning of the phenomena” (p. 51). After importing the audio and transcribed files into the research software, data analysis was conducted using the process steps described in the following sections.

Listing and preliminary grouping. Each transcribed interview was examined and bracketed for expressions relevant to the experience of decision-making uncertainty. During this initial analysis phase, according to Moustakas (1994), “the focus of the research is placed in brackets [and] everything else is set aside so that the entire research process is rooted solely on the topic and question” (p. 97). Referred to by Moustakas as *horizontalization*, this process required each relevant statement be treated with equal contextual value, bracketed into general units of meaning, and divided into preliminary groupings using epoché to set aside prejudgments. To accomplish this procedure within QSR NVivo 8, each transcript was saved as an internal source file and carefully read to identify broad, relevant statements and germane descriptions. The use of QSR NVivo 8 search, query, and statistical features further facilitated the identification of keywords and phrases relevant to the central research question.

During the initial review and evaluation of the interview transcriptions, the horizontalization process was broadly applied to the participants’ experiential descriptions to ensure a comprehensive listing of generally relevant statements and

expressions were identified. Each relevant statement was assigned to a descriptive label in order to parse and categorize the data for further analysis. The descriptive labels were coded as *free nodes* within QSR NVivo 8 as potential *horizons* of the experience.

Because the initial phase of the reduction process was encompassing and intentionally redundant, the approach yielded 4,528 *references* to 210 broadly defined descriptive labels (free nodes). Within QSR NVivo 8, a reference is a coded link between a relevant statement, expression, or key phrase to one or more free node. After conducting the preliminary grouping process, each transcribed interview contained an average of 215 references to an average of 75 free nodes.

The descriptive labels referentially coded to each relevant statement during the initial listing and preliminary grouping process represented generally defined horizons of the experience. Wilding and Whiteford (2005) suggested, “Each individual has a ‘horizon’ of understanding . . . [comprised of] the sum total of all influences that make individuals who they are, including the social, historical, and political contexts in which they live” (p. 101). Gilstrap (2007) noted that individuals perceive their experiences *on the horizon* based on their ability to understand complex phenomena. Through conversation and a mutual understanding of language, Gadamer (1989) argued that experiences are revealed through a “fusion of horizons” (p. 305). Therefore, the horizontalization process is inherently dependent on the comprehensive analysis of the transcribed discourse between the researcher and the participant (Langdridge, 2008).

Although horizons, according to Moustakas (1994) are “unlimited . . . as we can never exhaust completely our experience of things,” (p. 95) the phenomenological reduction process has diminished returns as the textual descriptions are analyzed for

understanding and meaning. Moustakas recommended the horizontalization process be discontinued when no additional distinctive characteristics or textual qualities associated with the phenomenon can be perceived. This “stopping point” corresponds to the thematic saturation point in which no new horizons emerge (Creswell, 2007; Guest et al., 2006; Moustakas, 1994). New horizons emerged from the first 18 interviews analyzed. Because no new horizons were revealed in the last three transcriptions analyzed, theoretical data saturation was confirmed.

Reduction and elimination. With the broad and generally defined horizons coded for each transcription, the purpose of the reduction and elimination phase of the data analysis process was to determine the *invariant constituents* (Moustakas, 1994). The invariant constituents are the unique and essential units of meaning that capture the textual qualities of the experience, enable understanding of the participants’ perspectives, and describe the distinctive characteristics of the central phenomenon (Moustakas, 1994). Moustakas (1994) developed two tests for each coded expression to extract the invariant constituents:

1. Does it contain a moment of the experience that is a necessary and sufficient constituent for understanding it?
2. Is it possible to abstract and label it? (p. 121)

These two tests, in the form of reflective questions, were applied to 1,579 coded expressions using QSR NVivo 8 to facilitate categorizing and linking the resulting constituents. Expressions meeting both criteria were coded as the essential horizons of the experience. Otherwise, the expression was eliminated. During this process, overlapping, repetitive, and vague expressions were eliminated as well. The remaining

horizons were the invariant constituents of the senior military officers' perceptions and experiences (Moustakas, 1994). The reduction and elimination procedure delimited the 210 broadly defined horizons originally identified during the horizontalization process to 87 invariant constituents. The 87 invariant constituents were coded as free nodes using exact descriptive terms designed to enhance the clustering and thematizing process. A summary of the invariant constituents in rank order is provided in Appendix J.

Clustering and thematizing the invariant constituents. Clustering the invariant constituents was conducted by analyzing QSR NVivo 8 data queries, node summary reports, and coding stripe density. Essential to the clustering process was Husserl's (1931) concept of *intentionality* in which consciousness and intuition combine to influence one's ability to make judgments (Moustakas, 1994). Intentionality includes "the act of perceiving, feeling, thinking, remembering, or judging" (i.e., noesis) and "that which is experienced" (i.e., noema; Moustakas, 1994, p. 69). Therefore, creating meaningful clusters was required to understand how the noesis directly related to the noema for each described experience.

The invariant constituents were clustered into thematic labels based on consistent associations and contextual relationships. The QSR NVivo 8 coding stripes substantially facilitated this process. The clustered thematic labels were identified as the core themes of the experience (Moustakas, 1994). Each key theme was coded as an individual *tree node* within QSR NVivo 8. The supporting invariant constituents for each core theme were placed under the associated tree node. The 10 key themes that emerged during the clustering and thematizing procedure are listed in Table 7. The key themes and supporting invariant constituents are listed in rank order in Appendix K. The core themes

and associated invariant constituents captured the collective essence of the senior military officers' perceptions and experiences describing the phenomenon (Moustakas, 1994).

Table 7

Key Themes

Key Theme Number	Key Theme Description
1	Response Characteristics and Efficacy Considerations
2	Social, Behavioral, Cultural, and Cognitive Aspects
3	Policy and Strategic Aspects
4	Legal and Ethical Aspects
5	Organizational Concepts, Constructs, and Relational Considerations
6	Data, Information, and Technology Considerations
7	Cyber Attack Characteristics
8	Cyber Warfare Characteristics
9	Cyberspace Characteristics
10	Experience, Training, and Education Considerations

Final identification of the invariant constituents and themes. The final identification of the invariant constituents and themes was accomplished using a comprehensive validation process. During this process, the key themes and associated invariant constituents were *validated* against each participant's interview digital recording, verbatim transcript, and field notes. The objective of the validation procedure was to ensure that contextual accuracy was not diluted or misrepresented by the clustering and thematizing process. Further, the relationships between the key themes and invariant constituents were verified for relevancy within the context of the participants' transcriptions. For each key theme and invariant constituent, validation was completed using the following inquiry process:

1. Are they expressed explicitly in the complete transcription?

2. Are they compatible if not explicitly expressed?
3. If they are not explicit or compatible, they are not relevant to the co-researcher's experience and should be deleted (Moustakas, 1994, p.121).

After the validation process was completed, the key themes were ranked based on the weighted average number of text segments coded to each invariant constituent. The "weights" were determined using the relative number of participants associated with the respective invariant constituent. The weighted average was considered the best metric for indicating thematic density of relevant contextual data (Landauer, Foltz, & Laham, 1998a, 1998b). Following are descriptions of the key themes identified and validated through review and analysis of the interview transcriptions.

Theme 1: Response characteristics and efficacy considerations. Theme 1 consisted of eight invariant constituents. The primary horizon was the lack of response options following a cyber attack. The participants described four response characteristics that influence decision-making uncertainty including response speed and responsiveness; target discrimination and distinction; response scalability; and autonomous response capability. The participants also described three considerations that influence response efficacy including response thresholds and necessity; proportionality and equivalence determination; and response process and authority. Theme 1 was characterized by 403 coded text segments and a weighted average text segment value of 65. Theme 1 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 2: Social, behavioral, cultural, and cognitive aspects. Theme 2 consisted of nine invariant constituents. The primary horizon was the extent of understanding cyber warfare. Other cognitive and behavioral horizons included the lack of common

lexicon and meaning; varied perceptions, values, and beliefs; and inadequate self-confidence. The participants described three cultural considerations including generational differences; military versus societal cultures; and academic versus commercial cultures. The participants also described two social factors influencing decision-making uncertainty including social and international norms, and dehumanizing cyber warfare. Theme 2 was characterized by 385 coded text segments and a weighted average text segment value of 61. Theme 2 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 3: Policy and strategic aspects. Theme 3 consisted of 11 invariant constituents. The primary horizons were an inadequate national strategic policy and the relative attribution level required to respond. Policy horizons included instrument of national power legitimacy; lack of deterrent consequences; untested rules of engagement; insufficient national resources and debate; lack of political resolve and transparency; and risk of escalation and cyber arms race. Strategic horizons included multiple actors and motives; operational gain versus intelligence loss; and current conflict posture considerations. Theme 3 was characterized by 527 coded text segments and a weighted average text segment value of 58. Theme 3 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 4: Legal and ethical aspects. Theme 4 consisted of eight invariant constituents. The primary horizon was the perception of an inadequate legal framework. Other legal horizons included sovereignty and jurisdiction challenges; privacy, anonymity, and civil liberty concerns; antiquated international treaties; and laws of armed conflict applicability. In addition to ethical warfare considerations, other ethical horizons

included hostile intent and act of war definitions, and ineffective governance, compliance, and controls. Theme 4 was characterized by 299 coded text segments and a weighted average text segment value of 52. Theme 4 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 5: Organizational concepts, constructs, and relational considerations.

Theme 5 consisted of six invariant constituents. This theme did not contain a predominate horizon. Two organizational concept horizons included ill-defined roles and responsibilities, and ambiguous leadership vision and accountability. Three organizational relationship horizons included lack of collaboration and consensus; ineffective command and control; and governmental stakeholders and conflicting equities. The remaining horizon was centralized versus decentralized constructs. Theme 5 was characterized by 229 coded text segments and a weighted average text segment value of 50. Theme 5 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 6: Data, information, and technology considerations. Theme 6 consisted of 11 invariant constituents. The primary horizon was poor understanding of current capabilities. Four information horizons included inconsistent information valuation and sharing; criminal activity versus information warfare; overly classified and compartmentalized; and lack of access and situational awareness. Three data horizons included proxies and identification authentication; forensic and data credibility challenges; and data ownership and intellectual property. Three technology horizons included immature modeling and simulations; inadequate technology exposure and utilization; and insufficient research and development. Theme 6 was characterized by

346 coded text segments and a weighted average text segment value of 49. Theme 6 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 7: Cyber attack characteristics. Theme 7 consisted of seven invariant constituents. This theme did not contain a predominate horizon. In addition to unintended higher order effects, six horizons describing cyber attack characteristics included recognition and categorization; severity determination; motive and context; kinetic attack analogy and equivalence; capacity and precision; and covertness and validity. Theme 7 was characterized by 251 coded text segments and a weighted average text segment value of 48. Theme 7 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 8: Cyber warfare characteristics. Theme 8 consisted of 12 invariant constituents. The primary horizon was complex EBO. The remaining 11 horizons describing cyber warfare characteristics included self-defense and counter attack; deconfliction and synchronization; traditional military activity extent; rules of war applicability; planning and targeting processes; damage assessment methods; fog of war and deception; integrating and normalizing operations; evolving level of readiness; catastrophic cyber event required; and irregular warfare and low cost of entry. Theme 8 was characterized by 374 coded text segments and a weighted average text segment value of 41. Theme 8 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 9: Cyberspace characteristics. Theme 9 consisted of nine invariant constituents. This theme did not contain a predominate horizon. The nine horizons describing cyberspace characteristics included ubiquitous domain of warfare; complex

and chaotic environment; critical infrastructure dependency; open and boundaryless commons; interdependent communication medium; insurgent area of hostility and crime; virtual and physical duality; ambiguous vulnerabilities; and levels of resiliency and security. Theme 9 was characterized by 277 coded text segments and a weighted average text segment value of 37. Theme 9 invariant constituents and textual data analysis are detailed in Appendix K.

Theme 10: Experience, training, and education considerations. Theme 10 consisted of six invariant constituents. This theme did not contain a predominate horizon. Three experience-based horizons included insufficient experience and expertise; poor anticipatory and proficiency skills; and undeveloped cyber warfare doctrine. Two training horizons included lack of formal training opportunities, and unrealistic and non-integrated exercises. The education horizon for this theme was the lack of institutional curricula regarding cyber warfare. Theme 10 was characterized by 162 coded text segments and a weighted average text segment value of 35. Theme 10 invariant constituents and textual data analysis are detailed in Appendix K.

Individual textual descriptions. Individual textual descriptions were used to summarize and portray each senior military officer's unique perceptions, thoughts, feelings, and insights regarding the uncertainty experienced when making decisions following a cyber attack. According to Moustakas (1994), the individual textual descriptions are constructed using the validated invariant constituents and key themes including verbatim examples when appropriate. The interview transcriptions, audio files, field notes, and the QSR NVivo 8 *coding by node* graphing feature were used to ensure contextual accuracy and validity. The process of creating individual textual descriptions

facilitated understanding “what” the senior military officers experienced. The individual textual descriptions for each participant are provided in Appendix L.

Individual structural descriptions. Individual structural descriptions were constructed from the participant’s respective textual descriptions by reflecting on the conditions that precipitated each experience. As the individual textual descriptions were developed, imaginative variation was used through the “acts of thinking and judging, imagining, and recollecting, in order to arrive at core structural meanings” (Moustakas, 1994, p. 79). Structures support textures as inherent causal foundations (Husserl, 1931). The goal of imaginative variation is to “seek possible meanings by utilization of imagination, varying the frames of reference, employing polarities and reversals, and approaching the phenomenon from divergent perspectives, different positions, roles or functions” (Moustakas, 1994, pp. 97-98). Accordingly, the individual structural descriptions, according to Moustakas (1994), provide a “vivid account of the underlying dynamics of the experience, the themes and qualities that account for ‘how’ feelings and thoughts connected with the phenomenon” (p. 135). The individual structural descriptions for each participant are provided in Appendix M.

Composite descriptions. The composite descriptions are an integrated construction of the senior military officers’ perceptions and lived experiences representing the group as a whole (Moustakas, 1994). Composite descriptions are created from the individual textual (see Appendix L) and structural (see Appendix M) descriptions. By incorporating the invariant constituents and key themes in a thoughtful and holistic manner, Moustakas (1994) found the meanings and essences of the experiences will emerge and reveal a comprehensive description of the phenomenon. By

developing the composite descriptions, Ihde (1977) asserted, “One moves from that which is experienced and described in concrete and full terms, the ‘what’ of the experience, towards its reflexive reference in the ‘how’ of the experience” (p. 50).

Although texture and structure are inherently coupled within the experience, Keen (1975) noted, “The interlocking of texture and structure does not preclude . . . focusing on one or the other at any given stage of phenomenological work” (p. 59).

The textual composite description was used to understand the *meaning* of the phenomenon; whereas, the structural composite description was used to expose the *essence* of the phenomenon. The structural composite description is constructed from the textual composite description using imaginative variation. The goal of this process, according to Moustakas (1994), is to “understand *how* the co-researchers as a group experience *what* they experience” (p. 142). Using the invariant meanings and core themes revealed in the individual descriptions is essential to this objective. The composite textual and structural descriptions are provided in Appendix N.

Textural-Structural synthesis. The textual-structural synthesis is the final step in the phenomenological reduction and analysis process (Moustakas, 1994). By combining the composite textural and structural descriptions of the decision-making uncertainty that senior military officers experience following a cyber attack, an integration and synthesis of the meanings and essences of the phenomenon was developed. The textual-structural synthesis is a “unity of texture and structure” (Moustakas, 1994, p. 151) of the phenomenon that describes the researcher’s understanding of *what* (texture) and *how* (structure) the experience occurred for the group as a whole. The textual-structural synthesis of the meanings and essences of central phenomenon is provided in Appendix

O. Five interdependent concepts (response process, human factors, governance, technology, and environment) that characterize the relationships between the key themes were revealed during the synthesis process. As a means of illustrating the integrated components of decision-making uncertainty following a cyber attack, these five overarching and interrelated components of uncertainty can be represented by a model similar to *Leavitt's Diamond* (Leavitt, 1965).

Summary

Chapter 4 included a presentation of the study findings that emerged from the exploration of perceptions and lived experiences of 21 senior military officers regarding their decision-making uncertainty following a cyber attack. The participants served for the CJCS at the Pentagon in Washington, DC. Data collection involved in-depth, semi-structured, conversational interviews using the following research question: *How do senior military officers perceive and describe the lived experience of decision-making uncertainty when determining the appropriate response to a cyber attack?* The interviews were digitally recorded, transcribed, coded, and analyzed using Moustakas' (1994) modification to the van Kaam (1959, 1966) method of analysis. QSR NVivo 8 qualitative research software was used to facilitate the phenomenological reduction process and observational field notes were used to capture the structural data.

During the exploration of the verbatim interview data from the 21 participants, 210 broadly defined horizons were identified from 1,579 expressions coded during horizontalization. The 210 general horizons were reduced to 87 invariant constituents (see Appendix J) by eliminating or combining overlapping, repetitive, and vague expressions. By clustering and thematizing the 87 invariant constituents, 10 key themes

(see Appendix K) emerged. Individual textual descriptions (see Appendix L) and individual structural descriptions (see Appendix M) were developed to support the construction of composite textual and structural descriptions (see Appendix N). The composite descriptions provided an enhanced understanding of *what* (texture) and *how* (structure) the participants, as a group, experienced the central phenomenon. Five interdependent relationships between the key themes consistently were revealed by synthesizing the meanings and essences of the experiences exposed in composite textual and structural descriptions (see Appendix O).

In chapter 5, conclusions and recommendations resulting from the data collected and analyzed in this qualitative, phenomenological study are presented. Conclusions are provided by aligning the purpose of this study with the data findings, the literature review, and the results of the composite textural-structural synthesis. In addition, the research study's scope and limitations are discussed. Implications and recommendations for leaders with respect to understanding the decision-making uncertainty following a cyber attack are offered. Chapter 5 is concluded with suggestions for future research.

Chapter 5: Conclusions and Recommendations

The United States is under attack in cyberspace (Carr, 2010; Clarke & Knake, 2010; Libicki, 2009). According to Defense Secretary Gates, we are “under cyber attack virtually all the time, every day” (Carr, 2010, p. 179). Escalating to cyber warfare occurs when cyber attacks are conducted as a strategic campaign for the primary purpose of affecting a nation’s societal behavior (Libicki, 2009). With over 140 countries possessing substantial cyber attack capabilities, cyber warfare is a substantial and ever-increasing threat to national security and international peace (Carr, 2010). General Cartwright added, “Cyberspace has emerged as a warfighting domain . . . and we are engaged in a less visible, but nonetheless critical battle against cyber attacks” (Owens et al., 2009, p.162). These considerations make timely and effective military response decisions imperative (Carr, 2010; Clarke & Knake, 2010; Owens et al., 2009). Therefore, the purpose of this qualitative, phenomenological research study was to explore the decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack.

The review of the literature indicated a need to gain better understanding of the decision-making uncertainties following a cyber attack (Michael et al., 2003; Owens et al., 2009; Phister et al., 2005; Tubbs et al., 2002; Waters et al., 2008; Wilson, 2007b). The literature review further showed minimal research regarding how national policy and legal frameworks (Carafano & Weitz, 2008; Kennedy, 2006; Owens et al., 2009; Wilson, 2008; Wingfield, 2009), leadership paradigms (Hansen, 2008; Kramer et al., 2007; Pace, 2006a), and decision theory (Keller & Yang, 2008; Owens et al., 2009; Shen et al., 2007; Wingfield, 2007) support cyber warfare decision-making. Because phenomenological

research designs are particularly effective at exposing, describing, and interpreting lived experiences and perceptions (Donalek, 2004; Goulding, 2005; Mitroff & Sagasti, 1973; Moustakas, 1994; Starks & Trinidad, 2007; van Manen, 1990), this current research study makes a substantive contribution to the body of knowledge regarding military leadership decision-making within a complex warfare environment.

The primary data collection method consisted of in-depth, semi-structured interviews guided by the research question: *How do senior military officers perceive and describe the lived experience of decision-making uncertainty when determining the appropriate response to a cyber attack?* Data analysis was conducted by employing Moustakas' (1994) modification to the van Kaam (1959, 1966) method of phenomenological reduction facilitated by QSR NVivo 8 software. The goal of data collection and analysis was to seek, rigorously transcribe, and accurately code the individual participant's perceptions and insights in order to reveal the meanings and essences of the lived experiences, providing a comprehensive understanding of the phenomenon that represents the group as a whole.

In chapter 5, the data findings presented in chapter 4 are interpreted. Following a review of the scope, limitations, and delimitations, conclusions are drawn from the literature review and the data analysis including a conceptual model of the interdependent relationships between the key themes. Implications are presented that indicate the research significance in general and for leadership. Recommendations are made for leaders with the goal of better understanding the decision-making uncertainty following a cyber attack. Chapter 5 is concluded with recommendations for further research and a summary.

Scope

The scope of this study was focused on senior military officers serving in cyber warfare divisions on the Joint Staff at the Pentagon in Washington, DC. Military officers who serve on the Joint Staff are screened and assigned specifically based on their outstanding military careers including lived experiences of warfare decision-making (M. D. Johnson, personal communication, June 12, 2009). Because the specific sample size for qualitative research methods cannot be predetermined to exact precision, sufficient interviews were conducted to ensure no new key themes emerged (Groenewald, 2004; Moustakas, 1994; van Manen, 1990). For typical phenomenological research studies, approximately 20 participants are required to reach thematic saturation (Boyd, 2001; Creswell, 2007; Luborsky & Rubenstein, 1995). For this study, the phenomenological reduction process showed theoretical saturation was reached after 18 interviews with the analysis of three additional interviews confirming this conclusion.

Limitations

Limitations of a study are the boundaries and qualifications outside the control of the researcher (Creswell, 1994; Kornuta & Germaine, 2006). First, this phenomenological research study was limited to participants who volunteered to participate, the amount of time available to conduct the study, and the reliability of the research instrument (interview process). Second, the sample was limited to senior military officers with specialized cyber warfare decision-making experience. Based on the participant's lived experiences and responsibilities, the third limitation allowed only cyber attacks against DoD information systems to be considered.

The final limitation was associated with the interview process. Because the participants were not equally articulate, self-reflective, or expressive, the researcher's military warfare experience could have introduced limitations based on personal bias and perceptual distortions (Creswell, 2005; Moustakas, 1994). However, by applying *epoché* during the interview process and by bracketing the research topic during data coding, the researcher's potential bias associated with preconceived notions and judgments about decision-making uncertainty was minimized (Bednall, 2006; Moustakas, 1994).

Delimitations

Delimitations are intentional boundaries placed on the study to narrow the scope and to make the study more manageable (Kornuta & Germaine, 2006; Leedy & Ormrod, 2010). This research study was delimited by three constraints. First, the interviews were confined to senior military officers serving on the Joint Staff in cyber divisions in Washington, DC. For this study, senior military officers were defined as Army, Navy, Air Force, and Marine Corps officers in pay grades O5 (Lieutenant Colonels or Commanders) and above. Second, the participants were asked to consider only cyber attacks against computer systems, networks, and information technology infrastructures that service the GIG and the DIB. By only considering GIG and DIB information systems during the interview process, confusion associated with the DoD's existing lines of authority and areas of responsibility was minimized. Finally, the research study content, including the interview questions and responses, was restricted to unclassified descriptions, events, scenarios, tactics, techniques, and procedures not associated with the official position of any U.S. government department or agency.

Conclusions

Research conclusions were drawn from the analysis and synthesis of in-depth, semi-structured interview data collected from 21 senior military officers serving for the CJCS in Washington, DC by employing Moustakas' (1994) modification to the van Kaam (1959, 1966) method of phenomenological reduction. The data collected was in response to the lead interview question: *Please describe the decision-making uncertainty you experience when determining the appropriate response to a cyber attack.* The conclusions were based on 87 invariant constituents and 10 key themes that emerged from 210 broadly defined horizons identified from 1,579 coded textual expressions. By constructing individual textual and structural descriptions and synthesizing the composite textual-structural descriptions, the core themes and associated invariant constituents indicated five primary topical areas that represent the decision-making uncertainty the participants experienced as a group following a cyber attack.

A synthesis of the composite textual-structural descriptions showed consistent perceptual and experiential relationships between the key themes. The relationships were categorized into five distinct and interrelated components: (a) response process, (b) human factors, (c) governance, (d) technology, and (e) environment. The *response process* component was supported by three key themes: response characteristics and efficacy considerations (Theme 1); cyber attack characteristics (Theme 7); and cyber warfare characteristics (Theme 8). The *human factors* component was supported by two key themes: social, behavioral, cultural, and cognitive aspects (Theme 2); and experience, training, and education considerations (Theme 10). The *governance* component was supported by two key themes: policy and strategic aspects (Theme 3); and legal and

ethical aspects (Theme 4). The *technology* component was supported by one key theme: data, information, and technology considerations (Theme 6). The *environment* component was supported by two key themes: organizational concepts, constructs, and relational considerations (Theme 5); and cyberspace characteristics (Theme 9). The factors that influence decision-making uncertainty and the supporting key themes are illustrated by the conceptual model shown in Figure 6.

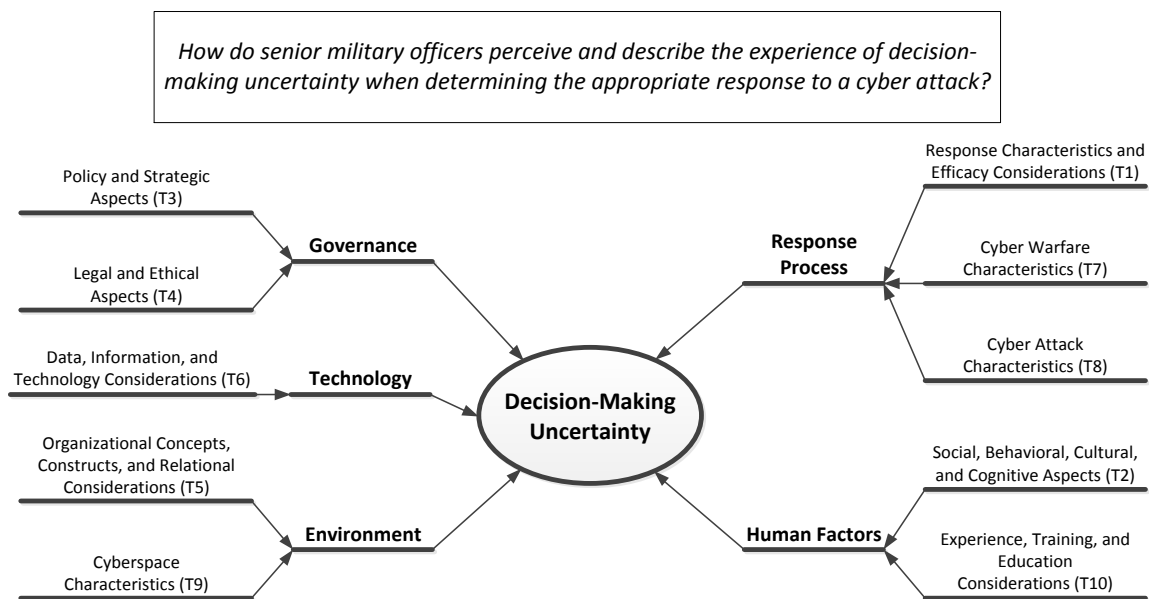


Figure 7. Conceptual model representing the factors influencing decision-making uncertainty following a cyber attack with ranked themes shown in parentheses.

The final step of Moustakas' (1994) modification to the van Kaam (1959) method of phenomenological reduction requires the construction and synthesis of a composite textural-structural description of the central phenomenon by incorporating the invariant constituents and key themes. The purpose of this step was to create an integrated and comprehensive depiction of the meanings and essences of the participants' experiences. Because the conclusions that follow are based on findings from the synthesized

composite textual-structural description, the label “participants” is used to represent the group as a whole. Findings from the review of the literature were compared to the research conclusions noting similarities, differences, and gaps when applicable.

Response process. The response process is comprised of a highly complex set of operations, activities, and events requiring an in-depth understanding and mastery of cyber warfare tactics, techniques, and procedures. The participants confirmed the literature finding that the complexity of the existing response process contributes to the decision-making uncertainty experienced following a cyber attack (Carr, 2009; Clarke & Knake, 2010; Kugler, 2009; Obama, 2009; Owens et al., 2009). The senior military officers in this study described the response process based on response characteristics and efficacy considerations, cyber warfare characteristics, and cyber attack characteristics.

Response characteristics and efficacy considerations. The participants expressed the decision to respond to a cyber attack is made uncertain by the lack of response options. The literature review indicated this uncertainty is compounded by ill-defined response thresholds (“red lines”) preventing the determination of *necessity* in accordance with the laws of armed conflict (Libicki, 2009; Rattray, 2001; Wingfield, 2006). Because response thresholds are not properly defined, the participants conveyed the decision-making process is unresponsive, untimely, and ineffective. The participants confirmed the literature findings that indicated determining a *proportional* response to a cyber attack within an equivalent traditional warfare context is challenging (Kennedy, 2006; Schmitt, 1998, 1999, 2002).

The participants found the response process to be impeded further by ambiguous lines of authority at the operational level. The participants added that response options

lack scalability, which severely limits the ability to respond effectively to the large range of cyber attack severities encountered. The review of the literature showed the inability to scale and tailor responses to attacks in cyberspace is complicated by the technical challenges associated with cyber target *distinction* and *discrimination* (Peng, Wijesekera, et al., 2006; Schmitt, 2002; Wingfield, 2006). Noting the need to distinguish cyber targets accurately and timely, the participants relayed how developing and incorporating better autonomous response capabilities that adequately address less severe, high-density cyber attacks would reduce decision-making uncertainty. The efficacy of automatic response systems using an active-defense approach is documented in the literature (Michael et al., 2003; Owens et al., 2009; Wingfield et al., 2005).

Cyber attack characteristics. The senior military officers in this study expressed a concern that responding to a cyber attack could result in unintended and undesirable higher order effects. The participants' concerns confirmed the literature review findings associated with the complexity of determining second and third order effects (Cebrowski, 2002; O'Donnell & Kraska, 2002). Specifically, the decision to respond to a cyber attack is made less certain when considering the potentially detrimental and uncontrolled cascading events that might result (Atkinson & Moffat, 2005; Butler et al., 2005; Wilson, 2007b). The participants found their apprehensions regarding higher order effects to be exacerbated by the inability to recognize and categorize the source and severity of cyber attacks using consistent and reproducible methods.

Because cyber attacks are often conducted in a covert manner, the participants found validating how the attack occurred to be overly difficult, untimely, and complex. Adding to the complexity, the participants described their abilities to discern and

understand the motive and context of a cyber attack as inadequate. The review of the literature indicated a contextual understanding of an adversary's attack motive is essential to the decision-making process and the development of an effective deterrence policy (Kugler, 2002, 2009; Saunders & Levis, 2007; Smith, 2006). Additionally, the participants noted that accurately determining an adversary's cyber attack capacity (e.g., botnet size and scope) and precision (i.e., surgical strike characteristics with minimal collateral damage) is challenging. To reduce decision-making uncertainty, Michael et al. (2003) suggested using a measured process such as the Schmitt analysis (Schmitt, 1998) to express a cyber attack with equivalent kinetic attack characteristics.

Cyber warfare characteristics. The participants described cyber warfare as a set of traditional military activities comprised of complex EBO well suited for national self-defense and for conducting counter attacks during hostile conflicts. Unfortunately, the participants conveyed deconflicting and synchronizing cyber operations are exceedingly complicated due to cumbersome planning and targeting processes further impeded by conflicting interagency equities. These complications hinder integrating and normalizing cyber warfare into mainstream military operations (Carr, 2010; Clarke & Knake, 2010; Pace, 2006a). Consistent with the literature review, the participants found applying the conventional rules of war in cyberspace to be challenging and not straightforward (Sharp, 1999a; Smith, 2006; Wingfield et al., 2005).

The participants expressed that decision-making uncertainty is strongly influenced by the "fog of war" created in cyberspace resulting from advanced deception capabilities and methods. The complexity of cyber warfare is catalyzed by the low cost of entry into this domain (compared to traditional warfare), which provides an inexpensive medium

for non-state adversaries to conduct attacks (Ahamad et al., 2008; Carafano & Weitz, 2008; Wilson, 2007b). Consequently, cyber warfare should be categorized as a type of irregular warfare from a doctrinal perspective (Kehler, 2009; Miller, 2000). The participants perceived the readiness and willingness of DoD senior leaders to respond to the spectrum of cyber attacks were evolving.

The participants believed accurately conducting “battle damage” assessments following a cyber attack is impeded by undefined information valuation standards (i.e., clear, consistent, and generally accepted expression of the *worth* of information). The review of the literature indicated comprehensive damage assessments are essential for making informed business, policy, and warfare decisions (Phister et al., 2005; Sanders & Levis, 2007; Schechtman, 1997; Schmitt, 2006). Without fully understanding the equivalent damage caused by cyber attacks, contextualizing cyber warfare among different stakeholders within a common frame is challenging. Given this challenge, the participants suggested a catastrophic cyber event (“Cyber 9/11”) would likely occur before interagency leaders or the general population seriously consider cyber warfare a substantial threat to national security. The literature findings were divided on the plausibility of a “digital Pearl Harbor” event occurring (Stohl, 2007; Wilson, 2008).

Human factors. Human factors include cognitive properties, social behaviors, skills and abilities, organizational cultures, human-machine interaction, learnability, procedural and technology usability, and other related categories that enhance decision-making processes (Carroll, 1997). The participants confirmed the literature finding that an integrated compilation of human factors influences the decision-making uncertainty experienced following a cyber attack (Endsley, 1995; Saunders & Levis, 2007; Smith,

2006; Stanton et al., 2004; Wallenius, 2005). The senior military officers in this study described the effects that human factors have on decision-making based on social, behavioral, cultural, and cognitive aspects as well as experience, training, education considerations.

Social, behavioral, cultural, and cognitive aspects. The participants conveyed the need for an improved level of individual understanding regarding the complex dynamics, interrelated effects, and decision-making processes associated with cyber warfare. The literature review indicated that understanding cyber warfare is limited currently by the lack of a common lexicon and an inconsistent vernacular (Kramer et al., 2007; Kuehl, 2008; Smith, 2006). The participants added that developing a common understanding would be challenging due to the diverse values and belief systems from the numerous stakeholders with equities in cyberspace. Consistent with the literature, the participants expressed that insufficient knowledge levels negatively affect their self-confidence and ability to make sound response decisions (Butler et al., 2005; O'Donnell & Kraska, 2002; Pace, 2006a).

Generational differences (i.e., cultural and ideological variances resulting from differences in age) add to the decision-making uncertainty following a cyber attack (Bartholomees, 2008; Smith, 2003). The participants believed Admirals and Generals (Baby Boomers) view cyberspace much differently than Lieutenants (Millennials). Further, substantive differences between the military and society's views of cyberspace are evident in the literature (Bartholomees, 2008; Brachman, 2006; Brey, 2006). The participants explained how the military views cyberspace as an operational domain of business and warfare, whereas society views cyberspace as a social network medium for

collaborating and communicating. The literature review also showed marked differences between the academic (free exchange of ideas) and commercial (ideas exchanged for profit) viewpoints of cyberspace (Han, 2003; Hansen, 2008; Knapp & Boulton, 2006). The diversity in the various cultural perspectives, according to the participants, creates ideological tension and decisional disparity when assessing battle damage and the effects of a response in cyberspace.

Regarding the social nature of cyberspace, existing international norms of behavior influence the decision-making process based on what is perceived as the acceptable bounds of response options (Beidleman, 2009; D. Denning, 2007; Goure, 2008). Consistent with the literature, the participants found social norms of behavior affect large policy decisions such as deterrence and response thresholds (Callaghan & Kauffman, 2008; Libicki, 2009; Taipale, 2009). As the line between social and virtual realities continues to blur, physical and digital identities become indistinguishable to human perception (Deutsch, 1995; Fox et al., 2009; Turkle, 1984, 1995). Therefore, the evolving social paradigm reinforces the belief that digital personas are actual representations of their human counterparts.

This virtual coupling, according to the participants, creates uncertainty when determining a response to a cyber attack. To address this problem, the participants asserted policies and rules of engagement should be developed that relegate cyber attacks to *machine versus machine* in order to achieve the proper perspective regarding depersonalizing cyber responses. By *dehumanizing* cyber warfare, the uncertainty in making challenging response decisions is reduced. The review of the literature indicated

the decision-making efficacy of decoupling virtual and physical identities within a cyber warfare context to be a new finding not previously studied.

Experience, training, and education considerations. The participants described their experience and expertise in cyber warfare for making effective response decisions as insufficient compared to the expected skill levels in traditional warfare domains.

Inadequate expertise is attributed to the lack of formal training opportunities during the normal career progression of senior officers and the absence of cyber warfare curricula at higher-level DoD universities and educational institutions (Gates, 2010a; Hansen, 2008; Libicki, 2009).

Because of the nascent and burgeoning nature of cyber warfare, the current doctrine governing cyber warfare tactics, techniques, and procedures is underdeveloped and not well understood (Gates, 2010a; Hansen, 2008; Owens et al., 2009; Pace, 2006a). Aggravating this problem, according to the participants, is the lack of leadership support to develop and integrate realistic and challenging exercise scenarios into existing war games and simulations. The participants confirmed the literature review findings that simplistic exercises and the lack of relevant doctrine have prevented developing a robust experience base (Carr, 2010; Saunders & Levis, 2007; Smith, 2006). Without improved training and education opportunities, the participants opined their anticipatory and proficiency skills would be inadequate to combat sophisticated cyber threats with respect to making timely and effective response decisions.

Governance. The governance structure is a system of rules, regulations, policies, laws, and traditions by which authority is exercised. The governance spectrum is comprised of (a) strategic ends, ways, and means, (b) political vision and policy

directives, and (c) laws, treaties, and ethical activities. The participants confirmed the literature finding that each component along the governance spectrum influences the decision-making uncertainty experienced following a cyber attack (Bartholomees, 2008; Carr, 2010; Kennedy, 2006; Obama, 2009; Owens et al., 2009; Schmitt, 1999, 2002; Wegener et al., 2003). The senior military officers in this study described how the governance structure affects decision-making based on policy, strategic, legal, and ethical aspects of cyber warfare.

Policy and strategic aspects. The participants believed that the national strategic policy regarding cyber warfare is inadequate to make effective response decisions. The lack of national policy limits the viable and credible consideration of using cyberpower as a legitimate instrument of national power (Bartholomees, 2008; Kramer et al., 2007; Kuehl, 2009; Pace, 2006a). Further adding to the policy challenges, the participants contended that the level of attribution certainty required to respond to a cyber attack is arbitrary and unrealistically ambitious. The technical challenges associated with achieving a high degree of attribution confidence impede the desire to establish and firmly declare deterrent consequences (Beidleman, 2009; Libicki, 2009; Taipale, 2009). Compounding the problem of developing an effective cyber deterrence policy, according to the participants, is the number and types of global actors with competing equities and motives in cyberspace.

The senior military officers in this study emphasized that the rules of engagement for responding to cyber attacks are nascent and generally untested. Without clear and meaningful rules of engagement, operational commanders do not have well defined lines of authority to exercise their inherent right of self-defense (Schmitt, 1998, 1999; Sharp,

1999a; Wingfield, 2006; Wingfield & Michael, 2004). Adding complexity to the self-defense calculus, cyber response decisions are complicated by the tradeoffs between operational gain and intelligence loss (Butler et al., 2005; Owens et al., 2009; Pace, 2006a). According to the participants, these tradeoffs are complicated further by the lack of political resolve and insufficient transparency among interagency partners, especially within the intelligence community.

Insufficient national resources and debate have been applied to cyber concepts and capabilities resulting in cyber warfare policy and doctrine that remain relatively immature compared to other nation states (Libicki, 2009; Owens et al., 2009; Saunders & Levis, 2007; Wilson, 2008). Consistent with the review of the literature, the participants expressed concerns that the current resourcing priority associated with developing and acquiring cyber attack capabilities is inadequate to defend the nation against emerging threats (Ahamad et al., 2008; Obama, 2009; Owens et al., 2009). Given that the decision to respond to any attack, cyber or kinetic, is influenced heavily by the existing conflict posture and capability advantage, the participants agreed with the literature that any overt response could needlessly increase the risk of escalating hostilities while unintentionally stimulating a cyber arms race (Reid, 2007; Taipale, 2009; Tubbs et al., 2002).

Legal and ethical aspects. The participants considered the existing legal framework governing the use of force in cyberspace to be antiquated and inadequate to support military operations in an effective manner. The literature was inconsistent regarding the adequacy of the current legal framework with respect to cyber response decisions. From a strictly international law perspective, the literature review indicated the legal framework is sufficient when a cyber attack can be represented by equivalent

kinetic attack characteristics (Schmitt, 1998, 1999; Sharp, 1999a; Wingfield, 2007). In this case, the literature review showed the laws of conflict management (*jus ad bellum*) and the laws of armed conflict (*jus in bello*) are adequate and can be used to govern the use of force in cyberspace (Schmitt, 2002; Wingfield, 2009; Wingfield & Michael, 2004).

Conversely, from an operational practitioner's perspective, the participants contended the legal framework does not address sovereignty challenges, jurisdiction boundary problems (e.g., cloud computing, transborder data flows, etc.), non-state actors, severity thresholds, and the technical nuances of cyber attacks (Carr, 2010; Joyner & Lotrionte, 2001; Owens et al., 2009; Wingfield, 2006). Although the participants confirmed the literature review finding that cyber warfare is a completely ethical use of force, the lack of practical definitions for hostile intent and hostile act in cyberspace make consistently responding to cyber attacks difficult (D. Denning, 2007; Owens et al., 2009; Rowe, 2007; Schmitt, 1998). While noting these definitional problems, the participants maintained that antiquated international treaties and the unpredictable societal view of cyber warfare complicate determining how to apply the laws of armed conflict in cyberspace.

Compounding these challenges, the participants expressed domestic laws add uncertainty to the response decision-making process. Consistent with the literature review, the participants submitted privacy, anonymity, and civil liberty concerns have not been addressed within a cyber warfare context (Sharp, 1999b; Wegener et al., 2003; Wilson, 2008). Building on these issues, the participants noted the inability for appropriate agencies to enforce compliance with existing laws and technical standards has failed to provide effective governance and controls for malicious activities in

cyberspace. The perceived lack of enforcement was confirmed by the literature review (Kennedy, 2006; Sharp, 1999b; Silver, 2002; Taipale, 2009; Wegener et al., 2003).

Technology. For this research study, technology was considered information systems and supporting capabilities used to facilitate the practical application of knowledge. The participants confirmed the literature finding that the reluctance to develop, embrace, and apply technology influences the decision-making uncertainty experienced following a cyber attack (Bartholomees, 2008; Cabana, 2000; Carr, 2010; Owens et al., 2009; Schmitt, 1998; Tubbs et al., 2002). The senior military officers in this study described how technology affects decision-making based on data and information system considerations.

Data, information, and technology considerations. The participants conveyed their deficient understanding of current technical capabilities contributes to the uncertainty they experience when making cyber response decisions. Additionally, the participants confirmed the literature review findings that information valuation standards and information sharing mechanisms are inconsistent across the U.S. government and private sectors (Atkinson & Moffat, 2005; Gates, 2010a; Obama, 2009; Pace, 2006a). These inconsistencies, according to the participants, make determining the scope and impact of a cyber attack challenging. The participants further concluded that the lack of information sharing, which frequently results from insufficient network access due to improper classification and compartmentalization procedures, reduces situational awareness and the development of a common operating picture among stakeholders (Obama, 2009; Smith, 2003, 2006).

Compounding the information sharing problems, the participants explained how technical challenges impede the ability to make timely response decisions. Specifically, the widespread use of proxies (i.e., misleading virtual identities), immature forensic capabilities, and weak identification authentication measures make attributing malicious cyber activity difficult (Chaikin, 2007; Saunders & Levis, 2007; Wheeler & Larsen, 2007). Furthermore, the technical and legal difficulties associated with integrity and ownership of data in transit coupled with complex intellectual property rights increase the uncertainty of response decisions, especially when data servers reside in the United States. Additionally, the review of the literature indicated that predictive models and realistic simulations are required to understand the effects of cyber attacks more fully (Moffat, 2003; Power, 2007; Shen et al., 2007). The participants attributed the lack of models and simulators to insufficient resources for research and development at the national laboratory level.

Environment. The environment is a system of interdependent settings, boundaries, conditions, objects, and circumstances encountered when making response decisions. The environment contains physical (tangible interfaces), organizational (cultural and relational interfaces), and virtual (cyber interfaces) components. The participants confirmed the literature finding that environmental factors influence the decision-making uncertainty experienced following a cyber attack (Clarke & Knake, 2010; Knapp & Boulton, 2006; Libicki, 2009; Nunes, 1999; Saunders & Levis, 2007; Wegener et al., 2003). The senior military officers in this study described how environmental factors affect decision-making based on organizational concepts, constructs, and relationships as well as cyberspace characteristics.

Organizational concepts, constructs, and relational considerations. The participants expressed that the lack of collaboration and consensus, especially among U.S. government departments and agencies, creates decision-making uncertainty following a cyber attack. In addition to external organizational challenges, the participants contended that ineffective command and control processes and ill-defined roles and responsibilities within key military organizations also add complexity to response decisions. With respect to military organizations, the participants confirmed the literature review findings that both centralized and decentralized command and control structures are required for responding to the vast number of cyber attack methods and source locations (Atkinson & Moffat, 2005; Saunders & Levis, 2007; Smith, 2003). Many government stakeholders with conflicting equities in cyberspace further complicate the synchronization and response decision process following a cyber attack (Atkinson & Moffat, 2005; Bush, 2003; Gallinetti et al., 2006; Obama, 2009). Consequently, the participants believed ambiguous leadership, ineffective oversight, and weak accountability measures confound the deconfliction problem and prevent streamlined decisions from being made.

Cyberspace characteristics. The participants described cyberspace as a ubiquitous domain of warfare embedded within a highly complex and chaotic environment. Furthermore, the participants characterized cyberspace as an open and essentially boundaryless commons designed primarily as an interdependent communication medium. With respect to emerging threats, the participants considered the existing levels of network resiliency and security to be inadequate, making cyberspace vulnerable to increased attacks and malicious behavior. As indicated by the literature review, these

characteristics considerably contribute to the decision-making uncertainty following a cyber attack (Dinstein, 2002; Kuehl, 2009; Owens et al., 2009; Pace, 2006a).

Extending the applicability of counterinsurgency operations, the participants suggested that the ever-increasing dependency of the nation's critical infrastructure on cyberspace creates opportunities for "cyber insurgents" to conduct hostile and criminal activities. The concept of conventional insurgents using cyberspace to hide their identities while covertly conducting malicious activities is well documented (Brachman, 2006; Thomas, 2006; Webster, 2010). However, the review of the literature indicated the idea of *purely* cyber insurgents using virtual identities (e.g., avatars, proxies, guilds etc.) through social networking or gaming sites for the purposes of conducting cyber warfare has not been studied to any extent.

The concept of cyberspace is complicated further by the complex duality of its virtual and physical nature (Kuehl, 2009; Pace, 2006a; Saunders & Levis, 2007; Turkle, 1984, 1995). This inherent characteristic, according to the participants, creates unique cyberspace vulnerabilities, confounds understanding higher order effects when making response decisions, and complicates deconflicting traditional military activities from intelligence gathering activities. The participants stressed they often experience indecision when attempting to optimize the competing efforts between CNA, CND, and CNE without clear guidelines and policy directives. The literature review showed the indecision that results from equally appealing alternatives is governed by the *choice uncertainty principle* (P. Denning, 2007). The review of the literature further indicated that applying the choice uncertainty principle to cyber warfare decision-making processes has not been studied.

Structural Framework for Understanding Decision-Making Uncertainty

Five main interrelated areas (response process, human factors, governance, technology, and environment) were shown categorically to describe the overall decision-making uncertainty experienced by senior military officers when determining the response to a cyber attack. These five areas of uncertainty were revealed during the textural-structural synthesis of the composite descriptions while conducting Moustakas' (1994) modification to the van Kaam (1959, 1966) method of phenomenological data analysis. The relationships between the five interdependent components that characterize the 10 key themes of this phenomenological study can be represented by a modified Leavitt's Diamond (Leavitt, 1965; Radnor, 1999).

Structural framework. Leavitt (1965) originally described an organization as a dynamic system comprised of four variables: tasks (service and operations), technology (tools), people, and structure (organizational). Figure 7 illustrates this original construct. In this model, Leavitt considered an organization as an open system that operates dynamically with its environment. Furthermore, the four variables are interdependent; therefore, a change in one variable affects the others (Smith, Norton, & Ellis, 1992; Radnor & Boadan, 2004). Leaders are responsible for directing and managing the four variables to minimize the uncertainty that accompanies organizational change (Smith et al., 1992; Radnor & Boadan, 2004). According to Smith et al. (1992), Leavitt's Diamond was used to illustrate the need to approach organizational change from a balanced perspective by understanding the complex interactions and forces between the key variables.

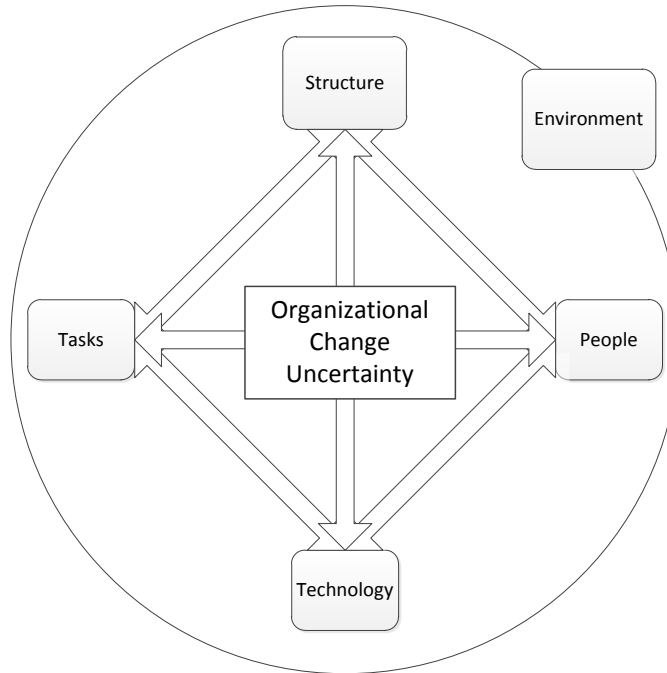


Figure 8. Leavitt's (1965) Diamond for modeling organizational change.

Radnor (1999) updated Leavitt's Diamond with terms that are more recognizable based on current management research and language. Consequently, Radnor and Boadan (2004) constructed their model using strategy, processes, people, and technology as the corners of the diamond. In this modification to Leavitt's model, *strategy* represents the vision and objectives providing direction and policy to the organization. The *process* variable signifies the mechanics, structure, and systems of the organization. The *people* variable captures the culture, motivation, training, and education aspects of the organization. The *technology* variable indicates the software, hardware, and information technology systems used by the organization to manage data, information, and knowledge (Radnor & Boadan, 2004).

The current research study showed Radnor's (1999) modification to Leavitt's (1965) Diamond can be used as a structural framework for describing the decision-making uncertainty experienced by senior military officers following a cyber attack. The

synthesis of the textual-structural descriptions indicated that the five interdependent topics representing the 10 key themes of this study (see Figure 6) were closely related to the variables that Radnor used to modify Leavitt's original model. Figure 8 illustrates this structural framework.

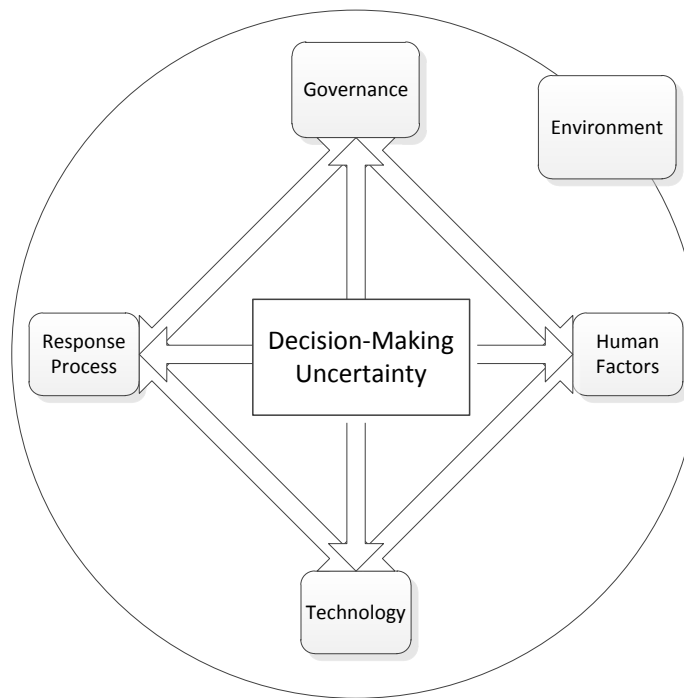


Figure 9. Radnor's (1999) modified Leavitt Diamond applied to the interdependent factors representing the decision-making uncertainty senior military officers experience following a cyber attack.

The relationship between uncertainty and organizational change is documented in the literature (Bordia, Hobman, Jones, Gallois, & Callan, 2004; Bordia, Hunt, Paulsen, Tourish, & DiFonzo, 2004; DiFonzo & Bordia, 1998; Herzig & Jimmieson, 2006). Brashers (2001) explained, "Uncertainty exists when details of situations are ambiguous, complex, unpredictable, or probabilistic; when information is unavailable or inconsistent; and when people feel insecure in their own state of knowledge or the state of knowledge

in general” (p. 478). Within the organizational context, uncertainty is categorized at three levels: external (e.g., environment and technological), organizational (e.g., structure and culture), and individual (e.g., task, process, roles, and responsibilities; Bordia, Hobman, et al., 2004).

The sources of uncertainty during organizational change are unclear strategic vision, inefficient transformation processes, lack of transparency and information flow, and ineffective communication between stakeholders (Bordia, Hobman, et al., 2004). By comparison, the similarities between the findings of this research study regarding decision-making uncertainty and the sources of organizational change uncertainty are apparent. The review of the literature supported this assertion and reinforced the structural framework components (see Figure 8) that depicted this study’s findings (Bordia, Hobman, et al., 2004; Bordia, Hunt, et al., 2004; Brashers, 2001; DiFonzo & Bordia, 1998; Keen, 1981; Tversky & Kahneman, 1974).

Poliheuristic decision-making process. The findings of this research study indicated the existing decision-making process used by senior military officers was best described by poliheuristic decision theory. The literature review indicated that poliheuristic decision theory was used frequently to explain use of force decisions made by leaders within complex environments in which the higher order effects of the decision are too interrelated and complicated to be determined by analytical methods alone (James & Zhang, 2005; Keller & Yang, 2008; Mintz, 1993, 2004, 2005). Poliheuristic decision theory is characterized by a two-stage process (Mintz, 2004). First, the set of decisional alternatives is reduced by a noncompensatory process in which heuristics (e.g., mental “thumb rules” developed with experience) eliminate options with unacceptable outcomes

based on political, diplomatic, military, or economic dimensions or criteria (James & Zhang, 2005; Mintz, 2004). Second, the remaining alternatives are evaluated using more analytical methods as the means of making a final decision that minimizes risk and maximizes benefits (Mintz, 2004).

The phenomenological reduction process indicated several invariant constituents that support the assertion that the decision-making uncertainty that senior military officers experience following a cyber attack is described most comprehensively by poliheuristic decision theory. Specifically, senior military officers described the decision-making process as a complex effects-based operation within a multifaceted and chaotic environment in which operational gain versus intelligence loss must be considered when balancing risk. These judgments require experience and intuition, among other rational elements of cognition such as critical thinking (James & Zhang, 2005). Further, the participants described how the decision-making process must consider strategic political and ethical military criteria while minimizing unintended higher order effects when employing cyberpower as an instrument of national power (Chesser, 2007). Finally, the participants shared that the response decision relies heavily on precise attack recognition, categorization, and attribution capabilities and analytical techniques (DeRouen & Sprecher, 2004).

Implications

The research study's conclusions yielded implications for two primary stakeholder organizations, notably the DoD and the NSC. With respect to cyber warfare, the DoD is responsible for "providing reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities,

natural disasters, and accidents” (England, 2009, p. 2) consistent with federal laws and regulations. The DoD is further responsible for ensuring the GIG is properly configured, managed, and operated in order to support strategic priorities and operational objectives in cyberspace. The DoD coordinates with the DHS to accomplish its cyber roles and responsibilities including securing, safeguarding, and protecting the nation’s critical infrastructure and DIB (Gates, 2010a; Napolitano; 2010).

Since its inception under President Truman, the NSC has served as “the principal forum for considering, advising, and assisting the president on national security and foreign policy matters . . . [and] for coordinating these policies among various government agencies” (National Security Council, 2010, para. 1). In addition to the President (chair), the NSC is comprised of national security advisors and cabinet officials including the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, and the National Security Advisor. The CJCS is the statutory military advisor to the NSC and the Director of National Intelligence is the intelligence advisor. Originally stemming from the National Security Act of 1947, the NSC’s authority has been amended, revised, and implemented by law, executive order, or policy directive under each president (Brown, 2008). With respect to cyberspace, the NSC’s roles and responsibilities are centered on implementing a national cybersecurity strategy that “improves resilience to cyber incidents and reduces the cyber threat” (National Security Council, 2010, para. 4).

Implications for the Department of Defense. Each key theme of this research study had implications for the DoD. Of most importance, improved response options with clearly defined thresholds and lines of authority are necessary to reduce decision-

making uncertainty following a cyber attack (Carr, 2009; Libicki, 2009; Owens et al., 2009). The senior military officers in this study admitted to having inadequate understanding of cyber warfare principles and capabilities. Exacerbating this problem is the lack of formal cyber warfare doctrine and a joint lexicon of common terms and equivalent definitions based on other warfighting domains (Kramer et al., 2007; Kuehl, 2006; Smith 2006).

Decision-making following a cyber attack is complicated by outdated and untested rules of engagement (Korns & Kastenberg, 2008; Owens et al., 2009; Pace, 2006a; Saunders & Levis, 2007). Further, the senior military officers participating in this study described the uncertainty that results from ambiguously defined tradeoffs between operational gain and intelligence loss when making response decisions. In addition, practical legal interpretations of how key concepts such as sovereignty, hostile intent, and law of armed conflict apply in cyberspace hamper effective decision-making processes (Carr, 2010; Joyner & Lotrionte, 2001; Owens et al., 2009; Wingfield, 2006).

The creation of USCYBERCOM (Gates, 2010b) has improved reducing the uncertainty resulting from previously ill-defined roles and responsibilities across numerous disparate command and control structures (Gates, 2010a; Libicki, 2009). However, delegation rules and policies regarding cyber warfare authority inherent to decentralized combatant commands remain lacking (Atkinson & Moffat, 2005; Saunders & Levis, 2007; Smith, 2003). Organizational changes and new policies require effective leadership and clear directives to ensure implementation plans are effective (Obama, 2009; Saunders & Levis, 2007; Smith 2006).

The senior military officers participating in this study conveyed they have insufficient understanding of current cyber capabilities due to overly classified and compartmentalized information. The participants expressed their situational awareness following a cyber attack is hindered further by inadequate access to real time information via a common operating picture. Adding to these challenges, fully understanding the higher order effects that result from responding to a cyber attack is marginalized by undeveloped “battle damage” assessment methods, target discrimination capabilities, and the lack of predictive models (Moffat, 2003; Smith 2003, 2006; Wallenius, 2005). Furthermore, the level of cyber warfighting experience and expertise among senior military officers requires improvement because of the lack of formal training and education opportunities (Gates, 2010a; Hansen, 2008; Tubbs et al., 2002).

Implications for the National Security Council. The lack of a comprehensive national strategy that unites and focuses cybersecurity efforts across the interagency reduces the effectiveness of responding to a cyber attack (Bush, 2003; Obama, 2009; Owens et al., 2009; Pace, 2006a). Fundamental to this problem is the absence of a clear, declaratory policy that highlights and broadly defines the United States’ national security posture regarding cyber attacks to the international community (Beidleman, 2009; Kugler, 2009; Libicki, 2009). Unlike nuclear deterrence policy, the firm establishment of consequences coupled with the political resolve to execute those consequences following a cyber attack has not been demonstrated. Normalizing cyberpower into the arsenal of other instruments of national power (i.e., diplomatic, information, military, economic, etc.) should be imperative. Additionally, the fear of a cyber arms race or escalating cyber

retaliation resulting from implementing and conveying a robust national cybersecurity policy is unfounded (Goure, 2008; Kugler, 2009; Wilson, 2008).

The national policy void further discounts an antiquated legal framework that is already ill equipped to address complex cyber attack challenges due to privacy and civil liberty concerns (Carr, 2010; Owens et al., 2009; Sharp, 1999b). Without applying consistent national resources toward cyber capability development and fostering healthy debate over response thresholds and act of war definitions in cyberspace, the decision-making uncertainty following a cyber attack will not expeditiously improve (Kennedy, 2006; Owens et al., 2009; Wegener et al., 2003). Without insightful, experienced, and presidentially empowered leadership, the deconfliction and synchronization processes between U.S. government stakeholders with competing equities will remain dysfunctional (Bush, 2003; Obama, 2009; Pace, 2006a). Absent strong leadership, the occurrence of a catastrophic cyber event (“Cyber 9/11”) will likely have to occur before cyber threats and vulnerabilities are considered a national agenda item.

Significance of the Study

This research study yielded insights about decision-making uncertainty through the perceptions and lived experiences of senior military officers who make cyber warfare decisions. For this study, research significance included advancing the body of knowledge of cyber warfare and making decisions under conditions of uncertainty within complex environments. The review of the literature showed substantial research had been conducted on the legal, technical, and policy aspects of cyber warfare (Obama, 2009; Schmitt, 1998, 1999; Sharp, 1999a; Silver, 2002; Wilson, 2007a, 2007b; Wingfield, 2006). However, research studies designed to explore the effectiveness of

existing legal and policy frameworks as applied to actual cyber attack scenarios were lacking in the literature (Carr, 2010; Clarke & Knake, 2010; Kramer et al., 2007; Owens et al., 2009).

Although considerable research was evident on decision-making processes to use force during traditional warfare (DeRouen, 2000; Meernik, 1994; Mintz, 1993, 2004, 2005; Ostrom & Job, 1986), the literature review indicated the absence of research studies associated with making cyber warfare decisions (Owens et al., 2009; Phister et al., 2005; Saunders & Levis, 2007; Wilson, 2007b). First, the predominant military leadership paradigm lacks an understanding of the dimensions and nature of cyber warfare (Butler et al., 2005; Keller & Yang, 2008; Lewis et al., 2008; Pace, 2006a). Second, a lack of research on applying existing decision theories to cyber warfare decision-making processes was evident. Specifically, a clear literature gap exists with respect to understanding how leaders make decisions to use force in response to cyber attacks (Butler et al., 2005; Carr, 2010; Hansen, 2008; Keller & Yang, 2008; Shen et al., 2007).

In support of adding to the body of knowledge of cyber warfare and determining the associated leadership implications, the structural framework shown in Figure 8 is the culmination of the findings and conclusions of this research study. The interdependent relationships between the five main topics that represent the 10 key themes of this research study are displayed by this framework using a modified Leavitt's (1965) Diamond. Synthesis of the research findings showed remarkable similarities between the factors that described the senior military officers' decision-making uncertainty and the general variables associated with organizational change management (Brashers, 2001;

Bordia, Hobman, et al., 2004; Bordia, Hunt, et al., 2004; DiFonzo & Bordia, 1998; Herzig & Jimmieson, 2006; Keen, 1981; Nadler & Tushman, 1980; Tversky & Kahneman, 1974). Therefore, the relationship between cyber warfare decision-making uncertainty and organizational change management is an important research conclusion of this study.

The literature review indicated a void in the research regarding the social, cognitive, behavioral, and ethical implications and considerations when making decisions to use force in cyberspace (Beidleman, 2009; Bitzinger, 2009; D. Denning, 2007; Halpin et al., 2006). These characteristics emerged in the current research study during the data analysis as invariant constituents. Furthermore, this research study supported the scarcity of research literature on understanding how existing decision theories apply to cyber warfare decision-making processes. The findings of the current research study indicated poliheuristic decision theory (James & Zhang, 2005; Keller & Yang, 2008; Mintz, 1993, 2004, 2005) best described how senior military officers determine the appropriate response to cyber attacks. This conclusion is an important research finding and was based on a comprehensive evaluation and thorough comparison of the invariant constituents to the characteristics of the various decision theories described in chapter 2.

Significance to Leadership

The literature review indicated the necessity for “senior leadership across the U.S. government to work toward a common understanding and appreciation of the critical need to coordinate and develop clear offensive and defensive policy for making operational decisions within the cyber domain” (Saunders & Levis, 2007, p. 4). The findings, conclusions, and implications of this research study contribute to the DoD

leadership's awareness and understanding of the decision-making uncertainty experienced by senior military officers when determining the appropriate response to a cyber attack. The relationship between response process, human factors, governance, technology, and environment that emerged from the synthesis of the composite textual-structural descriptions may inform leadership policy decisions regarding response thresholds, rules of engagement, and lines of authority. By better understanding the uncertainties associated with cyber warfare decision-making, the operational readiness of combatant commanders is improved and the effectiveness and timeliness of their response decisions are enhanced (Hansen, 2008; Mathers, 2007).

Additionally, NSC leaders may use the findings of this research study to develop a declaratory cyber deterrence policy designed to dissuade cyber attacks supported by the use of cyberpower as an instrument of national power (Kramer et al., 2007; Kugler, 2009; Taipale, 2009). Furthermore, understanding the perspectives of senior military officers regarding the lack of coordination and collaboration between U.S. government agencies and departments may stimulate NSC leaders to improve deconfliction and synchronization processes following a cyber attack (Bush, 2003; Obama, 2009; Pace, 2006a). Given the ever-increasing number of cyber attacks that occur globally, military leaders and national security decision-makers worldwide may find the results of the current study useful for improving their understanding of cyber warfare policies and response decision processes (Beidleman, 2009; Mathers, 2007; Vamosi, 2007).

Recommendations for Leaders and Stakeholders

The recommendations are based on the structural framework of this research study (see Figure 8) and the associated implications for leaders and key stakeholders. As

previously described in the conclusions section and illustrated in Figure 6, the 10 key themes that emerged during the phenomenological data analysis for the current study were represented by the interdependent relationships between response process, human factors, governance, technology, and the environment (see Figure 8). The recommendations are provided for DoD and NSC leaders responsible for developing, implementing, and executing cyber warfare policies, strategies, and response decisions.

Recommendations for Department of Defense Leaders. In support of the actions being taken to operate effectively in cyberspace per the *Quadrennial Defense Review Report* (Gates, 2010a), *National Defense Strategy* (Gates, 2008), and *National Military Strategy for Cyberspace Operations* (Pace, 2006a), the following recommendations are made. In order to develop a more comprehensive approach to cyber warfare, the existing planning, targeting, and execution processes must be mainstreamed and normalized more fully into traditional military activities. This recommendation would require combatant commanders be provided more robust rules of engagement and enhanced cyber tactics, techniques, and procedures that are integrated into the spectrum of response options. Collaboration and coordination with interagency partners should be improved to deconflict and synchronize responses to cyber attacks more efficiently. Any effort to enhance collaboration following a cyber attack would be facilitated by improving information flow, data access, and situational awareness by properly (versus overly) classifying and compartmentalizing response options and capabilities.

As a means of developing better cyber expertise and awareness, senior military officers cannot be excluded. The normal tendency for the DoD is to build formal training

and education curricula into an officer's career path in order to "grow its cadre of cyber experts to protect and defend its information networks" (Gates, 2010a). Consequently, this method marginalizes senior decision-makers whose knowledge and understanding of cyber warfare, as shown by this research study, are already deficient. Therefore, applying a top-down approach to improving cyber expertise and knowledge levels among the senior officers serving for the CJCS and combatant commanders is recommended. This should include more rapidly developing cyber warfare doctrine and common terminology among the Services.

This research study indicated that conducting cyber warfare from a centralized command and control structure does reduce decision-making uncertainty. This finding was based on the senior military officers' existing understanding of response options, capabilities, and unintended higher order effects. However, as information flow, situational awareness, expertise, and collaboration with interagency partners improve due to the efforts currently being taken across the U.S. government (Gates, 2010a; Obama, 2009), the DoD should begin decentralizing cyber response authority to geographic combatant commanders where appropriate. This recommendation supports normalizing cyber warfare into traditional military activities as would be expected for any warfighting domain as the understanding and utilization of the respective capabilities evolve.

Recommendations for National Security Council Leaders. In support of the policies, programs, and initiatives being developed to enhance cybersecurity per the *National Security Strategy* (Obama, 2010), *Cyber Policy Review* (Obama, 2009), and *Securing Cyberspace for the 44th Presidency* (Lewis et al., 2008), the following recommendations are made. The NSC should develop and implement a national

declaratory policy regarding the United States' position on responding to cyber attacks. This policy should be based on international laws and treaties, be consistent with other declaratory response policies (e.g., WMD), and be written with general, non-provocative language. The findings of this research study indicated that the U.S. government has a moral and ethical responsibility to declare the expectation for appropriate behavior in cyberspace.

The goal of this declaration would be to promote and establish international norms consistent with the U.S. government's interpretive ideologies regarding sovereignty, privacy, and civil liberties. The declaratory policy would have the added benefit of deterring malicious activities, especially by legitimate nation states, to the maximum extent possible. Additionally, a firmly worded policy would cause cyber attacks to be viewed more generally as an equivalent kinetic attack within the context of existing international treaties and agreements governing armed conflict. This policy would form the fundamental directive for establishing the integrated, national cybersecurity strategy referred to in the *Cyberspace Policy Review* (Obama, 2009).

The NSC should take an active role in establishing response thresholds and in defining key concepts such as *hostile intent* and *hostile act* in cyberspace. These critical policy-based, legally informed definitions would reduce decision-making uncertainty by drawing a clearer line between operational gain and intelligence loss resulting from responding to cyber attacks. The NSC should establish clear leadership and recognized authority across the interagency in order to deconflict, synchronize, and coordinate response decisions. Finally, the NSC should legitimize cyberpower as a credible

instrument of national power without undue concerns over escalating cyber attacks or instigating a cyber arms race.

Recommendations for Further Research

Further research is recommended to continue the exploration of the decision-making uncertainty experienced when responding to cyber attacks and to validate the key themes, invariant constituents, and associated findings that emerged during the current study. Qualitative and quantitative approaches using different populations are recommended to explore the cyber warfare decision-making uncertainty phenomenon further and to investigate relevant topics shown to be lacking in the literature. The research recommendations in this section support broadening the limited scope of this qualitative, phenomenological study.

Validating the results off the current study. To validate the key themes and invariant constituents using different populations, repeating this qualitative, phenomenological study using senior military officers with cyber warfare expertise from other DoD organizations such as USSTRATCOM or USCYBERCOM is recommended. Conducting this study with senior officers from other military organizations would allow the results to be generalized more broadly. Because cyber warfare is nascent and rapidly evolving with respect to policy, doctrine, and expertise, the results of similar studies could yield marked differences in the results. As an alternative, conducting this phenomenological study with junior military officers as participants would be useful in exploring and contrasting the cultural variances in perceptions and lived experiences based on generational differences. Additionally, performing this phenomenological study with foreign military officers from a nation with similar cyber capabilities would be

valuable in understanding decision-making uncertainty through perspectives founded in different societal cultures, national policies, and legal frameworks.

Two noteworthy results of this study warrant additional research. First, future studies should investigate the relationship between the factors that influence cyber warfare decision-making uncertainty and organizational change management using response process, human factors, governance, technology, and environment as research variables. A quantitative research study is recommended that employs the theoretical model used by Bordia, Hobman et al. (2004) to test the relationship between decision-making uncertainty and organizational change management factors. The newly formed USCYBERCOM (Gates, 2010b) is recommended as a research platform based on the availability of respondents with cyber warfare expertise who recently experienced organizational change.

Second, a study should be conducted to examine the finding that the response process used by senior military officers following a cyber attack is described comprehensively by poliheuristic decision theory. A quantitative study is recommended that builds on the research conducted by Keller and Yang (2008) in which poliheuristic theory of decision-making (Mintz, 1993, 2004, 2005) was used to determine the “noncompensatory threshold” to use force during conflict. As an added benefit, the recommended study would be useful for DoD leaders who contend with the existing challenge of determining appropriate thresholds for responding to cyber attacks.

Addressing deficiencies in the literature. Further research is recommended in four areas to address literature gaps and limitations indicated by the review of the literature in support of findings associated with the current study. First, the literature

review showed mixed results regarding the plausibility of a large-scale cyber attack (“Cyber 9/11”) occurring against the nation’s critical infrastructure (Bartholomees, 2008; Stohl, 2007; Wilson, 2008). A Delphi study (Linstone & Turoff, 1975; Rowe & Wright, 1999) is recommended using a panel of DoD, DHS, private sector, and academic experts to improve understanding of the nation’s vulnerability to a wide scoping cyber attack and to forecast the probability of occurrence.

Second, the findings of the current study as validated by the literature review indicated a research need to understand the decision-making efficacy associated with dehumanizing cyber warfare. A quantitative study similar to Detert, Treviño, and Sweitzer’s (2008) research on moral disengagement in ethical decision-making is recommended. The research study should extend the work of Royakkers and van Est (2010) and Singer (2009) regarding the depersonalization of robotic warfare to cyber warfare.

Third, the idea of cyber insurgents using the Internet for covertly conducting cyber warfare was shown by the current study and the review of the literature to be a topic warranting additional research. Two research study approaches are recommended. A qualitative research study designed using content analysis of open source criminal investigation reports in which the characteristics of online predators are analyzed using counterinsurgency theory (Galula, 1964; Scott, 2008; Webster, 2010). Online predators (e.g., criminal, sexual, etc.) have been categorized as types of social networking insurgents (Choo, 2008; Marsico, 2010; Wade, 2003). The other recommendation is a qualitative research study using an ethnographic design in which Second Life (an Internet-based, 3-dimensional, virtual environment) is used as an immersive, interactive

platform. With this recommendation, the researcher monitors the participants, as avatars, within a social simulation using an agent-based model wherein certain participants are selected secretly to be cyber insurgents (Crooks, Hudson-Smith, & Dearden, 2009; Lee & Fang, 2009; Scott, 2008).

Finally, the current research study showed the participants experienced indecision resulting from the delicate balance between the operational gain and intelligence loss tradeoffs that occur when responding to cyber attacks. According to P. Denning (1985, 2007), such dilemmas are governed by the choice uncertainty principle in which the decision-maker is unable to select between equally attractive alternatives within a finite period. The review of the literature indicated the choice uncertainty principle as applied to cyber warfare had not been studied. A quantitative research study is recommended similar to the study conducted by Liu, Chen, Chen, and Sheu (2010) in which the choice uncertainty principle was applied to decisions made by information technology professionals regarding the indecision that results when equally appealing alternatives emerge during large software development projects.

Researcher's Reflections

Phenomenology is founded on the researcher's self-reflection, immersion, imaginative variation, and interpretation during the research process (Husserl, 1931; Moustakas, 1994; Priest, 2002; van Manen, 1990). Prior to conducting a phenomenological study, Patton (2001) recommended the initial reflection begin with the question: "What is my experience of this phenomenon and the essential experience of others who also experience this phenomenon intensely?" (p. 88). Therefore, by reflecting and intuiting on the phenomenon with the goal of understanding the essence and meaning

of the participants' lived experiences, the researcher used personal knowledge of the underlying problem to develop the research question and approach (Dowling, 2007; Priest, 2002). Because the researcher's experience, knowledge, and intuition are relied upon when conducting phenomenological research, the study results can be influenced by personal biases (Langdridge, 2008; Langfeldt, 2004; Wilding & Whiteford, 2005).

Given the essentiality of self-reflection while conducting phenomenological research, the researcher must remain aware of preexisting values and beliefs, prejudicial opinions, and biases that can affect the data collection, analysis, and interpretation of the findings (Starks & Trinidad, 2007). Langfeldt (2004) categorized research bias as either professional or personal. For the current study, the researcher's 26-year military career as a naval officer within the Submarine Force and previous assignment as the Assistant Deputy Director for Information and Cyberspace Policy for the CJCS were potential sources of professional bias. The researcher's thoughts and beliefs regarding warfare, use of force, and decision-making uncertainty were sources of personal bias. Unfortunately, both professional and personal biases can be detrimental to understanding the pure and unprejudiced essence of the phenomenon (Dowling, 2007).

During the current study, the researcher used several techniques to minimize the negative effects of professional and personal biases. First, the researcher did not subscribe or commit to a pre-existing theory prior to collecting and analyzing the data (Langdridge, 2006; Priest, 2002; Wilding & Whiteford, 2005). Second, the researcher used epoché during the face-to-face interviews and bracketing during the data analysis as means of suspending judgments and setting aside preconceived notions about the phenomenon (Bednall, 2006; Langdridge, 2006; Priest, 2002). Last, the researcher

rigorously and meticulously conducted each step of Moustakas' (1994) modified van Kaam method of phenomenological reduction with complete trust that the process would produce valid and reliable results (Groenewald, 2004; Hycner, 1985; Muto & Martin, 2009).

The researcher's experiences during the current study can be described as an emotional and intellectual life cycle. Emotionally, the doctoral journey began with a passionate commitment to make a substantive and significant contribution to the body of knowledge, followed by a sense of doubt and being overwhelmed, and ending with a renewed belief that the research process resulted in transformative growth as a scholarly leader and practitioner. Intellectually, the researcher began the doctoral process by leveraging a scientific and engineering background with a predominately positivistic and rationalistic viewpoint of epistemology. However, the challenges overcome while conducting this qualitative research broaden the researcher's intellectual aperture by revealing the epistemological value of interpretivism and constructivism perspectives.

Summary

In chapter 5, the conclusions of this study and associated implications for leaders were presented. The study's conclusions were based on 10 key themes that emerged from in-depth interviews with 21 senior military officers serving on the Joint Staff at the Pentagon in Washington, DC. The key themes and invariant constituents were determined using Moustakas' (1994) modification to the van Kaam (1959, 1966) method of phenomenological reduction and data analysis. A professional transcription service and QSR NVivo software facilitated the data analysis. Evaluating and synthesizing the key themes and invariant constituents revealed two important conclusions. First, the

decision-making uncertainty that senior military officers experience when determining the response to a cyber attack can be represented by a structural framework based on Radnor's (1999) adaptation of Leavitt's (1965) organization change management model. Second, the decision-making process used when responding to cyber attacks is described best by poliheuristic decision theory (DeRouen, 2000; Keller & Yang, 2008; Mintz, 1993, 2004, 2005; Mintz et al., 1994).

After a discussion of the study's significance to the research body of knowledge and to leadership, recommendations for reducing the decision-making uncertainty senior military officers experience following a cyber attack were made to DoD and NSC leaders. These recommendations were centered primarily on necessary policy and strategic changes, improving experience and situational awareness, and enhancing collaboration and coordination among the U.S. government departments and agencies. Chapter 5 was concluded with recommendations for future research. Future studies should be focused on expanding knowledge and gaining a better understanding of the more substantial findings of this study by validating the key themes and invariant constituents using similar and contrasting populations that are purposely selected.

References

- Abbate, J. E. (1994). *From ARPANET to Internet: A history of APRA-sponsored computer networks, 1966-1988* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 9503730)
- Addinall, R. (2004, October 29). *Information in warfare from Sun Tzu to the "war on terror."* Presented at the CDAI-CDFAI 7th Annual Graduate Student Symposium, Kingston, Ontario, Canada: Royal Military College.
- Ahamad, M., Amster, D., Barrett, M., Cross, T., Heron, G., Jackson, D., . . . Traynor, P. (2008, October 15). *Emerging cyber threats report for 2009: Data, mobility, and questions of responsibility will drive cyber threats in 2009 and beyond*. Retrieved from <http://www.dtic.mil/dtic/>
- Aiello, M. (2008). Social engineering. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber warfare and cyber terrorism* (pp. 191-198). Hershey, PA: Information Science Reference.
- Aikat, D. (1995). *Adventure in cyberspace: Exploring the information content of the World Wide Web on the Internet* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI Number: 9600582)
- Alexander, K. B. (2006, June). National information assurance (IA) glossary. *Committee on National Security Systems (CNSS) Instruction No. 4009*. Retrieved from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
- Alford, L. D. (2000). Cyber warfare: Protecting military systems. *Acquisition Review Quarterly, Spring*, 101-120. Retrieved from <http://www.dtic.mil/dtic/>

- Anderson, J., & Eppard, J. (1998). van Kaam's method revisited. *Qualitative Health Research*, 8(3), 399-403. doi:10.1177/104973239800800310
- Anderson, P. (1999). Complexity theory and organization science. *Organization Science*, 10(3), 216-232. doi:10.1287/orsc.10.3.216
- Andreessen, M., & Bina, E. (1994). NCSA Mosaic: A global hypermedia system. *Internet Research: Electronic Networking Applications and Policy*, 40(1), 7-17. doi:10.1108/10662241011059480
- Ashby, R. (1956). *An introduction to cybernetics*. New York, NY: John Wiley & Sons. Inc.
- Atkinson, P., Coffey, A., & Delamont, S. (2003). *Key themes in qualitative research: Continuities and change*. Walnut Creek, California: AltaMira Press.
- Atkinson, S. R., & Moffat, J. (2005). The agile organization: From informal networks to complex effects and agility. *Information Age Transformation Series Report*. Retrieved from <http://www.dtic.mil/dtic/>
- Avery, D. R., Tonidandel, S., Griffith, K. H., & Quinones, M. A. (2003). The impact of multiple measures of leader experience on leader effectiveness: New insights for leader selection. *Journal of Business Research*, 56(8), 673-679. doi:10.1016/S0148-2963(01)00312-5
- Ayson, R. (2000). Bargaining with nuclear weapons: Thomas Schelling's 'general' concept of stability. *The Journal of Strategic Studies*, 23(2), 48-71. doi:10.1080/01402390008437790
- Baldor, L. C. (2009, April 7). *Pentagon spends \$100 million to fix cyber attacks*. Retrieved from <http://www.physorg.com/print158333019.html>

Barnett, R. W. (1998, Spring). Information operations, deterrence, and the use of force.

Naval War College Review, 51(2), 7-19. Retrieved from <http://www.dtic.mil/dtic/>

Barnett, R. W. (2002). A different kettle of fish: Computer network attack. In M. N.

Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76*, pp. 21-33). Newport, RI: Naval War College.

Bartholomees, J. B. (2008, June). Volume I: Theory of war and strategy (3rd ed.). In

Guide to National Security Issues. Retrieved from <http://www.dtic.mil/dtic/>

Barzilai-Nahon, K., & Neumann, S. (2005, January 3). *Bounded in cyberspace: An*

empirical model of self-regulation in virtual communities. In *Track 7*. Presented at the 38th Hawaii International Conference on System Sciences, IEEE Computer Society.

Bednall, J. (2006). Epoché and bracketing within the phenomenological paradigm. *Issues*

in Educational Research, 16(2), 123-138. Retrieved from <http://www.eric.ed.gov/>

Beecham, S., Hall, T., Britton, C., Cottee, M., & Rainer, A. (2005). Using an expert panel

to validate a requirements process improvement model. *Journal of Systems and Software*, 76(3), 251-275. doi:10.1016/j.jss.2004.06.004

Beidleman, S. W. (2009). *Defining and deterring cyber war* (Master's thesis). U.S. Army

War College, Carlisle Barracks, PA.

Belknap, M. H. (2001, March 30). *The CNN effect: Strategic enabler or operational risk?*

Retrieved from <http://www.dtic.mil/dtic/>

Bell, D. E. (1982). Regret in decision-making under uncertainty. *Operations Research*,

30(5), 961-981. doi:10.1287/opre.30.5.961

- Bennet, A., & Bennet, D. (2008). The decision-making process for complex situations in a complex environment. In F. Burstein & C. W. Holsapple (Eds.), *Handbook on Decision Support Systems 1: Basic Themes* (pp. 3-20). Berlin: Springer-Verlag.
- Bentham, J. (1823). *An introduction to the principles of morals and legislation*. Oxford: Clarendon Press.
- Berg, B. L. (2004). *Qualitative research methods for the social sciences* (5th ed.). Boston, MA: Pearson.
- Berger, P. L., & Luckmann, T. (1966). *The social construction of reality*. New York, NY: Doubleday.
- Berners-Lee, T. (1989, March). *Information management: A Proposal*. Retrieved from <http://info.cern.ch/Proposal.html>
- Berners-Lee, T., & Cailliau R. (1990, November 12). *WorldWideWeb: Proposal for a hypertext project*. Retrieved from <http://www.w3.org/Proposal>
- Bernoulli, D. (1954). Exposition of a new theory on the measurement of risk. *Econometrica*, 22(1), 23-36. Retrieved from <http://www.jstor.org/>
- Bertalanffy, L. V. (1972). The history and status of general systems theory. *Academy of Management Journal*, 15(4), 407-426. Retrieved from <http://www.jstor.org/>
- Bettin, P. J., & Kennedy, J. K. (1990). Leadership experience and leader performance: Some empirical support at last. *Leadership Quarterly*, 1(4), 219-228. Retrieved from <http://www.elsevier.com/>
- Binnendijk, A. (1996). Conducting key informant interviews. *Performance Monitoring and Evaluation Tips*, 2(1-4). Retrieved from <http://www.dtic.mil/dtic/>

- Bitzinger, R. A. (2009). Arming the revolution in military affairs: The U.S. defense industry in the post-transformational world. *International Journal of Defense Acquisition Management*, 24, 17-31. Retrieved from <http://www.dtic.mil/dtic/>
- Blakesley, P. J. (2005). *Operational shock and complexity theory*. Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College.
- Blechman, B., & Kaplan, S. (1978). *Force without war: U.S. armed forces as a political instrument*. Washington, DC: Brookings Institution Press.
- Blum, K., & Muirhead, B. (2005). The right horse and harness to pull the carriage: Teaching online doctorate students about literature reviews, qualitative, and quantitative methods that drive the problem. *International Journal of Instructional Technology and Distance Learning*, 2(2), 29-45. Retrieved from <http://www.itdl.org/>
- Böhm, G., & Brun, W. (2008). Intuition and affect in risk perception and decision-making. *Judgment and Decision Making*, 38(10), 1-4. Retrieved from <http://www.ebscohost.com/>
- Bordia, P., Hobman, E., Jones, E., Gallois, C., & Callan, V. J. (2004). Uncertainty during organizational change: Types, consequences, and management strategies. *Journal of Business and Psychology*, 18(4), 507-532.
doi:10.1023/B:JOBU.0000028449.99127.f7
- Bordia, P., Hunt, E., Paulsen, N., Tourish, D., & DiFonzo, N. (2004). Uncertainty during organizational change: Is it all about control? *European Journal of Work and Organizational Psychology*, 13(3), 345-365. doi:10.1080/13594320444000128

- Borgmann, A. (2004). Is the Internet the solution to the problem of community? In A. Feenberg & M. Bakardjieva (Eds.), *Community in the Digital Age: Philosophy and Practice* (pp. 53-67). Lanham, MD: Rowman & Littlefield.
- Boyd, C. O. (2001). Phenomenology the method. In P. L. Munhall (Ed.), *Nursing research: A Qualitative Perspective* (3rd ed., pp. 93-122). Sudbury, MA: Jones and Bartlett.
- Boyd, J. R. (1976, September 3). *Destruction and creation*. Retrieved from http://www.goalsys.com/books/documents/destruction_and_creation.pdf
- Boyd, J. R. (1986, December). *Patterns of conflict*. Retrieved from <http://www.d-n-i.net/boyd/patterns.ppt>
- Boyd, J. R. (1996, January). *The essence of winning & losing*. Retrieved from <http://www.d-n-i.net/dni/strategy-and-force-employment/boyd-and-military-strategy/>
- Brachman, J. M. (2006). High-tech terror: Al-Qaeda's use of new technology. *The Fletcher Forum of World Affairs*, 30(2), 149-164. Retrieved from <http://fletcher.tufts.edu/forum/archives/pdfs/30-2pdfs/brachman.pdf>
- Brandt, W. C. (2006, March 15). *Preemption, 'red lines,' and international law - The legality of the 2002 national security strategy and a nuclear North Korea*. Retrieved from <http://www.dtic.mil/dtic/>
- Brashers, D. E. (2001). Communication and uncertainty management. *Journal of Communication*, 51(3), 477-497. Retrieved from <http://www.ebscohost.com/>
- Brehmer, B. (2005, June 13). *The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control*. Presented at the 10th

International Command and Control Research and Technology Symposium: The Future of C2, McLean, VA.

Brentano, F. C. (1874). *Psychology from an empirical standpoint*. Leipzig, Germany:

Duncker & Humblot.

Brey, P. (2006). Evaluating the social and cultural implications of the Internet. *SIGCAS*

Computers and Society, 36(3), 41-48. doi:10.1145/1195716.1195721

Brodie, B. (1946). *The absolute weapon: Atomic power and world order*. New York, NY:

Harcourt, Brace and Company.

Brodie, B. (1959). *Strategy in the missile age*. Princeton, NJ: Princeton University Press.

Brown, C. M. (2008). *The National Security Council: A legal history of the President's*

most powerful advisors (Project on National Security Reform, Ed.). Retrieved

from

<http://www.pnsr.org/data/images/the%20national%20security%20council.pdf>

Brumley, L., Kopp, C., & Korb, K. (2006). The orientation step of the OODA loop and

information warfare. In *7th Australian Information Warfare & Security*

Conference 2006 Proceedings (pp. 18-25). Presented at the Clayton School of

Information Technology, Monash University, Perth, Australia.

Bruno, G. (2008, February 27). *The evolution of cyber warfare*. Retrieved from

<http://www.cfr.org/publication/15577/>

Bryant, R., & Wilhite, A. (1990). Military experience and training effects on civilian

wages. *Applied Economics*, 22(1), 69-81. Retrieved from

<http://www.ebscohost.com/>

- Bryman, A. (1984). The debate about quantitative and qualitative research: A question of method or epistemology? *The British Journal of Sociology*, 35(1), 75-92.
Retrieved from <http://www.elsevier.com/>
- Bryman, A., Bresnen, M., Beardsworth, A., & Keil, T. (1988). Qualitative research and the study of leadership. *Human Relations*, 41(1), 13-30.
doi:10.1177/001872678804100102
- Bueno de Mesquita, B. (1981). *The war trap*. New Haven, CT: Yale University Press.
- Bueno de Mesquita, B. (1984). A critique of "A critique of the war trap." *Journal of Conflict Resolution*, 28(2), 341-360. Retrieved from <http://www.proquest.com/>
- Bueno de Mesquita, B. (2006). Game theory, political economy, and the evolving study of war and peace. *The American Political Science Review*, 100(4), 637-642.
doi:10.1017/S0003055406062526
- Bueno de Mesquita, B., & Lalman, D. (1990). Domestic opposition and foreign war. *American Political Science Review*, 84(3), 747-765. Retrieved from <http://www.jstor.org/>
- Bueno de Mesquita, B., & Lalman, D. (1992). *War and reason*. New Haven, CT: Yale University Press.
- Builder, C. H., Bankes, S. C., & Nordin, R. (1999). *Command concepts: A Theory derived from the practice of command and control*. Santa Monica, CA: RAND Corporation.
- Bull, S. (1991). *An historical guide to arms & armor*. Singapore: Random House.

- Bullock, R. K. (2006). *Theory of effectiveness measurement* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (ADA Number: 456717)
- Burnard, P. (2005). Interviewing. *Nurse Researcher*, 13(1), 4-6. Retrieved from <http://www.ebscohost.com/>
- Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organizational analysis*. Suffolk, UK: Ipswich Book Company.
- Bush, G. W. (2003, February). *The national strategy to secure cyberspace*. Retrieved from <http://www.dtic.mil/dtic/>
- Butler, R., Deckro, D., & Weir, J. (2005, Fall). Using decision analysis to increase commanders' confidence for employment of computer network operations. *IOSphere*, 33-38. Retrieved from <http://www.dtic.mil/dtic/>
- Cabana, N. C. (2000, April 4). Cyber attack response: The military in a support role. *Air & Space Power Online Journal*. Retrieved from <http://www.airpower.maxwell.af.mil/>
- Callaghan, J. P., & Kauffman, R. (2008). *Building cyber-security: The prospects of deterrence*. Retrieved from <http://www.dtic.mil/dtic/>
- Campbell, D. T., & McCormack, T. H. (1957). Military experience and attitudes toward authority. *The American Journal of Sociology*, 62(5), 482-490. Retrieved from <http://www.jstor.org/>
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the

- stock market. *Journal of Computer Security*, 11(3), 431-448. Retrieved from <http://ieeexplore.ieee.org/Xplore/>
- Cantwell, G. L. (2003). *Can two person zero sum game theory improve military decision-making course of action selection?* Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College.
- Carafano, J. J., & Weitz, R. (2008, February 8). Combating enemies online: State-sponsored and terrorist use of the Internet. *Backgrounder*, 2105, 1-9. Retrieved from <http://www.heritage.org/>
- Carr, J. (2010). *Inside cyber warfare*. Sebastopol, CA: O'Reilly Media, Inc.
- Carroll, J. M. (1997). Human-computer interaction: Psychology as a science of design. *Annual Review of Psychology*, 48, 61-83. doi:10.1006/ijhc.1996.0101
- Cartwright, J. E., Pace, P., & Rumsfeld, D. H. (2006, December). *Deterrence operations: Joint operating concept (v. 2.0)*. Retrieved from <http://www.dtic.mil/dtic/>
- Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004, April 1). The economic impact of cyber-attacks. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>
- Cassell, C., Buehring, A., Symon, G., & Johnson, P. (2006). Qualitative methods in management research: An introduction to the themed issue. *Management Decision*, 44(2), 161-166. doi:10.1108/00251740610650166
- Castro, A. D. (2003). Introduction to Giorgi's existential phenomenological research method. *Psicología desde el Caribe*, 11, 45-56. Retrieved from <http://www.jstor.org/>

- Cebrowski, A. K. (2002). CNE and CNA in the network-centric battlespace: Challenges for operators and lawyers. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76*, pp. 1-6). Newport, RI: Naval War College.
- Cerf, V. G. (1989). Requiem for the ARPANET. *ConneXions*, 38(10), 27. Retrieved from <http://www.connexionsjournal.org/>
- Chaikin, D. (2007). Network investigations of cyber attacks: The limits of digital evidence. *Crime, Law, and Social Change*, 46(4-5), 239-256.
doi:10.1007/s10611-007-9058-4
- Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. London, United Kingdom: Sage Publications.
- Chertoff, M. (2008, April 8). *Protecting our federal networks against cyber attacks*. Retrieved from http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm
- Chesser, N. (2007, October 1). Deterrence in the 21st century: An effects-based approach in an interconnected world. In (Strategic Multi-Layer Analysis Team, Ed.) *Volume I. U.S. Strategic Command Global Innovation and Strategy Center*. Retrieved from <http://www.dtic.mil/dtic/>
- Choo, K. K. R. (2008). Organized crime groups in cyberspace: A typology. *Trends in Organized Crime*, 11(3), 270-295. doi:10.1007/s12117-008-9038-9
- Churchman, C. W. (1967). Wicked problems. *Management Science*, 14(4), 141-142. Retrieved from <http://www.jstor.org/>
- Cioffi, J. (1997). Heuristics, servants to intuition, in clinical decision-making. *Journal of Advanced Nursing*, 26, 203-208. doi:10.1046/j.1365-2648.1997.1997026203.x

- Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do it*. New York, NY: HarperCollins Publishers.
- Clausewitz, C. V. (1873). *On war* (J. J. Graham, Trans.). London, United Kingdom: N. Trubner.
- Cohen, M., Etner, J., & Jeleva, M. (2008). Dynamic decision-making when risk perception depends on past experience. *Theory and Decision*, 64, 173-192.
doi:10.1007/s11238-007-9061-3
- Colaizzi, P. (1973). *Reflection and research in psychology: A phenomenological study of learning*. Dubuque, IA: Kendall-Hunt.
- Colaizzi, P. F. (1978). Psychological research as the phenomenologist views it. In R. S. Valle & M. King (Eds.), *Existential-phenomenological alternatives for Psychology* (pp. 48-71). New York, NY: Oxford University Press.
- Colby, E. (2007). Restoring deterrence. *Orbis*, 51(332), 413-428.
doi:10.1016/j.orbis.2007.04.004
- Coleman, K. G. (2007, November). Department of cyber defense: An organization who's time has come! *Technolytics*. Retrieved from <http://www.technolytics.com/>
- Coleman, K. G. (2008a, April 25). *Cyber attacks and cyber disasters: Are you prepared?*
Retrieved from <http://www.technewsworld.com/story/62725.html>
- Coleman, K. G. (2008b, May 27). *Russia's cyber forces*. Retrieved from <http://www.defensetech.org/archives/004200.html>
- Conger, J. A. (1998). Qualitative research as the cornerstone methodology for understanding leadership. *Leadership Quarterly*, 9(1), 107-121. Retrieved from <http://www.ebscohost.com/>

- Connolly, T., & Zeelenberg, M. (2002). Regret in decision-making. *American Psychological Society*, 11(6), 212-216. doi:10.1111/1467-8721.00203
- Conseil Européen pour la Recherche Nucleaire. (2008). *Where the web was born*. Retrieved from <http://public.web.cern.ch/Public/en/About/Web-en.html>
- Cooper, D. R., & Schindler, P. S. (2008). *Business research methods* (10th ed.). New York, NY: McGraw-Hill/Irwin.
- Correll, J. T. (1996). Warfare in the information age. *Air Force Magazine - Journal of the Air Force Association*, 79(12), 4-5. Retrieved from <http://www.dtic.mil/dtic/>
- Cowan, T. H. (1996). *A single flexible, rigorous decision making process*. Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College.
- Crane, D. M. (2002). Fourth dimensional intelligence: Thoughts on espionage, law, and cyberspace. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76)*, pp. 311-321). Newport, RI: Naval War College.
- Creswell, J. W. (1994). *Research design: Qualitative & quantitative approaches*. Thousand Oaks, CA: Sage Publications.
- Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd. ed.). Upper Saddle River, NJ: Merrill Prentice-Hall.
- Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

- Creswell, J. W. (2009). *Research design: Qualitative, quantitative and mixed method* (3rd ed.). Thousand Oaks, CA: Sage Publications.
- Crooks, A., Hudson-Smith, A., & Dearden, J. (2009). Agent street: An environment for exploring agent-based models in Second Life. *Journal of Artificial Societies & Social Simulation*, 12(4), 3-26. Retrieved from <http://www.ebscohost.com/>
- Crovitz, L. G. (2008, December 15). Internet attacks are a real and growing problem. *The Wall Street Journal*. Retrieved from <http://www.wsj.com/>
- Curran, K., Breslin, P., McLaughlin, K., & Tracey, G. (2008). Hacking and eavesdropping. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 307-317). Hershey, PA: Information Science Reference.
- Curran, K., Concannon, K., & McKeever, S. (2008). Cyber terrorism attacks. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 1-6). Hershey, PA: Information Science Reference.
- Czerwinski, T. J. (1998, January). Coping with the bounds: Speculations on nonlinearity in military affairs. *DoD Command and Control Research Program, Department of Defense*. Retrieved from <http://www.dtic.mil/dtic/>
- Dane, E., & Pratt, M. G. (2007). Exploring intuition and its role in managerial decision-making. *Academy of Management Review*, 32(1), 33-54. Retrieved from <http://www.ebscohost.com/>
- Davis, M. (2000). *The universal computer: The road from Leibniz to Turing*. New York, NY: W. W. Norton & Company, Inc.
- Dearnley, C. (2005). A reflection on the use of semi-structured interviews. *Nurse Researcher*, 13(1), 19-28. Retrieved from <http://www.ebscohost.com/>

Deken, J. M. (2006, May 31). *The early World Wide Web at SLAC (1991-1994)*.

Retrieved from <http://www.slac.stanford.edu/history/earlyweb/history.shtml>

Dellums, R. V., & Bingaman, J. (1993, March 29). *Defense industrial base: An overview of an emerging issue*. Retrieved from

http://cipp.gmu.edu/archive/513_GAOIndustrialBaseOverviewEmergingIssue_0393.pdf

Denning, D. E. (2007, March 27). *The ethics of cyber conflict*. Retrieved from

<http://www.nps.edu/faculty/dorothydenning/publications/Ethics%20of%20Cyber%20Conflict.pdf>

Denning, P. J. (1985). The science of computing: The arbitration problem. *American Scientist*, 73(6), 516-518. Retrieved from <http://www.americanscientist.org/>

Denning, P. J. (2007). The choice uncertainty principle. *Communications of the ACM*, 50(11), 9-14. doi:10.1145/1297797.1297809

Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods* (2nd ed.). New York, NY: McGraw-Hill.

DeRouen, K. (2000). Presidents and the diversionary use of force: A research note.

International Studies Quarterly, 44(2), 317-328. Retrieved from

<http://www.ebscohost.com/>

DeRouen, K., & Sprecher, C. (2004). Initial crisis reaction and poliheuristic theory.

Journal of Conflict Resolution, 48(1), 56-68. doi:10.1177/0022002703260271

Descartes, R. (1983). *Principles of philosophy* (V. R. Miller & R. P. Miller, Trans.).

Dordrecht, Netherlands: Kluwer Academic Publishers. (Original work published in 1644)

- Detert, J. R., Treviño, L. K., & Sweitzer, V. L. (2008). Moral disengagement in ethical decision-making: A study of antecedents and outcomes. *Journal of Applied Psychology, 93*(2), 374-391. doi:10.1037/0021-9010.93.2.374
- Deutsch, D. (1997). *The fabric of reality*. London, United Kingdom: The Penguin Press.
- DiFonzo, N., & Bordia, P. (1998). A tale of two corporations: Managing uncertainty during organization change. *Human Resource Management, 37*(3), 295-303. doi:10.1002/(SICI)1099-050X(199823/24)37:3/4<295::AID-HRM10>3.0.CO;2-3
- Dinstein, Y. (2002). Computer network attacks and self-defense. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76, pp. 99-120)*. Newport, RI: Naval War College.
- Dobrovolsky, J. L., & Fuentes, S. C. G. (2008). Quantitative versus qualitative evaluation: A tool to decide which to use. *Performance Improvement, 47*(4), 7-14. doi:10.1002/pfi.197
- Donalek, J. G. (2004). Phenomenology as a qualitative research method. *Urologic Nursing, 24*(6), 516-517. Retrieved from <http://www.ebscohost.com/>
- Dowling, M. (2007). From Husserl to van Manen: A review of different phenomenological approaches. *International Journal of Nursing Studies, 44*, 131-142. doi:10.1016/j.ijnurstu.2005.11.026
- Doyle, J. H. (2002). Computer networks, proportionality, and military operations. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76, pp. 147-162)*. Newport, RI: Naval War College.

- Drew, E. (2008, October 22). *Credit card companies' accomplices in millions of identity theft cases allege Eric Drew: Absence of verification safeguards allow thieves to steal*. Retrieved from <http://www.marketwatch.com/news/story/credit-card-companies-accomplices-millions/story.aspx>
- Drucker, P. F. (2007). *The effective executive*. Oxford: Elsevier Ltd.
- Easton, K. L., McComish, J. F., & Greenberg, R. (2000). Avoiding common pitfalls in qualitative data collection and transcription. *Qualitative Health Research*, 10(5), 703-707. doi:10.1177/104973200129118651
- Eberbach, E. (2005, August 31). *Decision theory = performance measure theory + uncertainty theory*. In *Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing*. Presented at the 10th International Conference, RSFDGrC 2005, Computer Science, Regina, Canada.
- Edwards, W. (1954). The theory of decision making. *Psychological Bulletin*, 51(4), 380-414. Retrieved from <http://www.ebscohost.com/>
- Edwards, W. (1961). Behavioral decision theory. *Annual Review of Psychology*, 12, 473-498. Retrieved from <http://www.ebscohost.com/>
- Einhorn, H. J., & Hogarth, R. M. (1981). Behavioral decision theory: Processes of judgment and choice. *Annual Review of Psychology*, 32, 53-88. Retrieved from <http://www.ebscohost.com/>
- Eldabi, T., Irani, Z., Paul, R. J., & Love, P. E. D. (2002). Quantitative and qualitative decision-making methods in simulation modeling. *Management Decision*, 40(1), 64-73. doi:10.1108/00251740210413370

- Elsea, J. K. (2006, August 11). Declarations of war and authorizations for the use of military force: Historical background and legal implications. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32-64. doi:10.1518/001872095779049543
- England, G. (2008a, May 12). *Defining cyberspace*. Deputy Secretary of Defense Action Memorandum. Retrieved from <http://www.dtic.mil/dtic/>
- England, G. (2008b, October 15). *Definition of cyberspace operations*. Deputy Secretary of Defense Action Memorandum (OSD 12681-08). Retrieved from <http://www.dtic.mil/dtic/>
- England, G. (2009, February 10). *Management of the Department of Defense information enterprise*. Retrieved from <http://www.dtic.mil/dtic/>
- Fagnot, I. J. (2008). Behavioral information security. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber warfare and cyber terrorism* (pp. 199-205). Hershey, PA: Information Science Reference.
- Farmer, T., Robinson, K., Elliott, S. J., & Eyles, J. (2006). Developing and implementing a triangulation protocol for qualitative health research. *Qualitative Health Research*, 16(3), 377-394. doi: 10.1177/1049732305285708
- Federal Communications Commission. (2007). Internet history: From ARPANET to broadband. *Congressional Digest*, 35-37. Retrieved from <http://www.ebscohost.com/>

- Fiedler, F. E. (1992). Time-based measures of leadership experience and organizational performance: A review of research and a preliminary model. *Leadership Quarterly*, 3(1), 5-23. doi:10.1016/1048-9843(92)90003-X
- Fishburn, P. C. (1989). Retrospective on the utility theory of von Neumann and Morgenstern. *Journal of Risk and Uncertainty*, 2(2), 127-158. Retrieved from <http://www.springerlink.com/>
- Fox, J., Arena, D., & Bailenson, J. N. (2009). Virtual reality: A survival guide for the social scientist. *Journal of Media Psychology*, 21(3), 95-113. doi:10.1027/1864-1105.21.3.95
- Frank, L. A. (1975, March-April). The decision to respond. *Air University Review*. Retrieved from <http://www.airpower.au.af.mil/>
- Fry, S. A. (2008, May 30). Department of Defense dictionary of military and associated terms. *Joint Publication 1-02*. Retrieved from <http://www.dtic.mil/dtic/>
- Gadamer, H. G. (1989). *Truth and method* (J. Weinsheimer & D. G. Marshall, Trans., 2nd ed.). London, United Kingdom: Continuum Publishing Group.
- Gallinetti, J. A., O'Bryan, M. S., & Ozolek, D. J. (2006, February 24). Commander's handbook for an effects-based approach to joint operations. *Joint Warfighting Center, U. S. Joint Forces Command*. Retrieved from <http://www.dtic.mil/dtic/>
- Galula, D. (1964). *Counter-insurgency warfare: Theory and practice*. New York, NY: Frederick A. Praeger.
- Gates, R. M. (2007, June 22). Pentagon cyber attack forces 1,500 PCs off line. *Pentagon Press Conference Transcription*. Retrieved from <http://www.foxnews.com/>

- Gates, R. M. (2008, June). *National defense strategy*. Retrieved from <http://www.dtic.mil/dtic>
- Gates, R. M. (2010a, February). *Quadrennial defense review report*. Retrieved from <http://www.dtic.mil/dtic/>
- Gates, R. M. (2010b, May 21). *DoD announces first U.S. Cyber Command and first U.S. CYBERCOM commander*. Retrieved from <http://www.defense.gov/releases/release.aspx?releaseid=13551>
- Gibson, W. (1984). *Neuromancer*. New York, NY: ACE Books.
- Gillies, J., & Cailliau, R. (2000). *How the web was born: The story of the world wide web*. Oxford: Oxford University Press.
- Gilstrap, D. L. (2007). Phenomenological reduction and emergent design: Complementary methods for leadership narrative interpretation and metanarrative development. *International Journal of Qualitative Methods*, 6(1), 95-113.
Retrieved from <http://creativecommons.org/>
- Giorgi, A. (1985). *Phenomenology and psychological research*. Pittsburgh, PA: Duquesne University Press.
- Giorgi, A. (2006). Concerning variations in the application of the phenomenological method. *The Humanistic Psychologist*, 34(4), 305-319.
doi:10.1207/s15473333thp3404_2
- Glaser, B. G. (1992). *Emergence versus forcing: Basics of grounded theory analysis*. Mill Valley, CA: Sociology Press.
- Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Hawthorne, NY: Aldine de Gruyter.

- Glenn, K. B. (2002). *"Complex" targeting: A complexity-based theory of targeting and its application to radical Islamic terrorism*. (Unpublished doctoral dissertation). Air Force Institute of Technology, Air University, School of Advanced Airpower Studies, Wright-Patterson Air Force Base, OH.
- Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4), 597-607. Retrieved from <http://www.proquest.com/>
- Goodman, C. M. (1987). The Delphi technique: A critique. *Journal of Advanced Nursing*, 12, 729-734. doi:10.1111/j.1365-2648.1987.tb01376.x
- Gorman, S. (2008, August 12). Georgia state's computers hit by cyber attack. *The Wall Street Journal*. Retrieved from http://www.afa.org/EdOp/edop_08-12-08.asp
- Goulding, C. (1998). Grounded theory: The missing methodology on the interpretivist agenda. *Qualitative Market Research*, 1(1), 50-57.
doi:10.1108/13522759810197587
- Goulding, C. (2005). Grounded theory, ethnography, and phenomenology: A comparative analysis of three qualitative strategies for marketing research. *European Journal of Marketing*, 39(3/4), 294-308. doi:10.1108/03090560510581782
- Goure, D. (2008, June 9). *Hunting for black swans: Military power in a time of strategic uncertainty*. Presented at the 2008 Air Force Strategy Conference, Scitor Corporation, Chantilly, VA: Lexington Institute.
- Gourley, B. (2008, May 29). *Towards a cyber deterrent*. Retrieved from <http://www.ctovision.com/cyber-deterrence-initiative.html>
- Grant, R. (2007, October). Victory in cyberspace. *The Air Force Association*. Retrieved from <http://www.dtic.mil/dtic/>

- Grisham, T. (2009). The Delphi technique: A method for testing and multifaceted topics. *International Journal of Managing Projects in Business*, 2(1), 112-130.
doi:10.1108/17538370910930545
- Groenewald, T. (2004). A phenomenological research design illustrated. *International Journal of Qualitative Methods*, 3(1), 42-55. Retrieved from <http://ejournals.library.ualberta.ca/>
- Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, 18(1), 59-82.
doi:10.1177/1525822X05279903
- Gurney, R. (2007, May 17). *NATO examines (Russian) cyber attacks on Estonia*. Retrieved from <http://www.altex-marketing.com/nato-examines-russian-cyber-attacks-on-estonia>
- Hall, W., & Callery, P. (2001). Enhancing the rigor of grounded theory: Incorporating reflexivity and relationality. *Qualitative Health Research*, 11(24), 257-272.
doi:10.1177/104973201129119082
- Halpin, E., Trevorrow, P., Webb, D., & Wright, S. (2006). *Cyberwar, netwar, and the revolution in military affairs*. New York, NY: Palgrave Macmillan.
- Han, K. H. (2003, May 23). *Cultural differences in cyberspace: Do traditional cultural dimensions fit into web communication contexts?* Presented at the 53rd Annual Conference of the International Communication Association, San Diego, CA.
- Hansen, A. P. (2008). *Cyber flag: A realistic cyberspace training construct* (Unpublished doctoral dissertation). Air Force Institute of Technology, Air University, School of Advanced Airpower Studies, Wright-Patterson Air Force Base, OH.

- Hansson, S. O. (2005, August 23). *Decision theory: A brief introduction*. Uppsala University, Department of Philosophy and the History of Technology, Royal Institute of Technology, Stockholm, Sweden. Retrieved from <http://www.infra.kth.se/~soh/decisiontheory.pdf>
- Hardmeier, S. (2005, August 25). *The history of Internet Explorer*. Retrieved from <http://www.microsoft.com/windows/ie/community/columns/historyofie.msp>
- Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4), 1008-1015.
doi:10.1046/j.1365-2648.2000.t01-1-01567.x
- Hastie, R., & Dawes, R. M. (2001). *Rational choice in an uncertain world: The psychology of judgment and decision-making*. Thousand Oaks, CA: Sage Publications.
- Hayek, F. A. (1964). The theory of complex phenomena. In M. Bunge (Ed.), *Critical Approaches to Science & Philosophy* (pp. 332-349). London, United Kingdom: The Free Press.
- Haywood, O. (1954). Military decision and game theory. *Journal of the Operations Research Society*, 2(4), 365-385. doi:10.1287/opre.2.4.365
- Hegel, G. W. F. (1807). *The phenomenology of mind* (J. B. Baillie, Trans.). London, United Kingdom: Macmillan Company.
- Heickerö, R. (2006, September 26). *Some aspects on cyber war faring in information arena and cognitive domain*. Presented at the 11th International Command and Control Research and Technology Symposium - Coalition Command and Control

in the Networked Era, Department of Homeland Security, Cambridge, United Kingdom.

Hertwig, R., Barron, G., Weber, E. U., & Erev, I. (2004). Decisions from experience and the effect of rare events in risky choice. *Psychological Science*, 15(8), 534-539. doi:10.1111/j.0956-7976.2004.00715.x

Herzig, S. E., & Jimmieson, N. L. (2006). Middle managers uncertainty management during organizational change. *Leadership & Organization Development Journal*, 27(8), 628-645. doi:10.1108/01437730610709264

Hildreth, S. A. (2001, June 19). Cyber warfare. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>

Holder, L. D., & Murray, W. (1998). Prospects for military education. *Joint Force Quarterly*, Spring, 81-90. Retrieved from <http://www.dtic.mil/dtic/>

Holland, J. H., & Miller, J. H. (1991). Artificial adaptive agents in economic theory. *Learning and Adaptive Economic Behavior*, 81(2), 365-370. Retrieved from <http://www.proquest.com/>

Holloway, I. (1997). *Basic concepts for qualitative research*. Malden, MA: Wiley-Blackwell.

Holosko, M. J. (2006). *Primer for critiquing social research: A student guide*. Florence, KY: Cengage Learning.

Holstein, J. A., & Gubrium, J. F. (1994). Phenomenology, ethnomethodology, and interpretative practice. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 262-272). Thousand Oaks, CA: Sage.

Howard, M. (1994-95). Lessons of the cold war. *Survival*, 36(4), 161-166.

doi:10.1080/00396339408442768

Hudson, D. (1997). *Rewired: A brief (and opinionated) net history* (1st ed.). Indianapolis,

IN: MacMillan Technical Publishing.

Hughes, R. B. (2009, February 24). *NATO and cyber defense: Mission accomplished?*

Retrieved from <http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf>

Husserl, E. (1931). *Ideas: General introduction to pure phenomenology* (W. R. B.

Gibson, Trans.). London, United Kingdom: George Allen & Unwin, Ltd.

Husserl, E., & Welton, D. (1999). *The essential Husserl: Basic writings in transcendental phenomenology*. Bloomington, IN: Indiana University Press.

Huurdemann, A. A. (2003). *The worldwide history of telecommunications*. Hoboken, NJ:

John Wiley & Sons. Inc.

Huynh, V. N., Nakamori, M., Ryoike, M., & Ho, T. (2007). Decision making under

uncertainty with fuzzy targets. *Fuzzy Optimization and Decision Making*, 6(3),

255-278. doi:10.1007/s10700-007-9011-0

Hycner, R. H. (1985). Some guidelines for the phenomenological analysis of interview

data. *Human Studies*, 8, 279-303. doi:10.1007/BF00142995

Ihde, D. (1977). *Experimental phenomenology*. New York, NY: G. P. Putnam Publishers.

International Federation of Operational Research Societies. (2006). IFORS' operational

research hall of fame: John von Neumann. *International Transactions in*

Operational Research, 13(1), 85-90. Retrieved from

<http://onlinelibrary.wiley.com/>

- James, P., & Oneal, J. R. (1991). The influence of domestic and international politics on the President's use of force. *Journal of Conflict Resolution*, 35(2), 307-332.
doi:10.1177/0022002791035002008
- James, P., & Zhang, E. (2005). Chinese choices: A poliheuristic analysis of foreign policy crises, 1950-1996. *Foreign Policy Analysis*, 1, 31-54. Retrieved from <http://www.proquest.com/>
- Janczewski, L. J., & Colarik, A. M. (2008). *Cyber warfare and cyber terrorism*. Hershey, PA: Information Science Reference.
- Jennex, M. E. (2008). Cyber war defense: Systems development with integrated security. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 241-253). Hershey, PA: Information Science Reference.
- Jervis, R. (1997). Complex systems: The role of interactions. In D. S. Alberts & T. J. Czerwinski (Eds.), *Complexity, global politics, and national security* (pp. 20-31). Washington, DC: National Defense University.
- Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, 24(4157), 602-611. doi: 10.2307/2392366
- Jonsen, K., & Jehn, K. A. (2009). Using triangulation to validate themes in qualitative studies. *Qualitative Research in Organizations and Management: An International Journal*, 4(2), 123-150. doi: 10.1108/17465640910978391
- Jordan, T. (1999). *Cyberpower: The culture and politics of cyberspace and the Internet*. New York, NY: Routledge.
- Josten, R. J. (2006, Summer). Strategic communication: Key enabler for elements of national power. *IOSphere*, 16-20. Retrieved from <http://www.dtic.mil/dtic/>

- Joyner, C. C., & Lotrionte, C. (2001). Information warfare as international coercion: Elements of a legal framework. *European Journal of International Law*, 12(5), 825-865. doi:10.1093/ejil/12.5.825
- Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263-291. Retrieved from <http://www.jstor.org/>
- Kampmark, B. (2007). Cyber warfare between Estonia and Russia. *Contemporary Review*, 289(1686), 288-293. Retrieved from <http://www.gale.cengage.com/>
- Kant, I. (1764). *Inquiry concerning the distinctness of the principles of natural theology and morality* (D. Walford & R. Meerbote, Trans., Immanuel Kant, Theoretical Philosophy 1755-1770). Cambridge, MA: Cambridge University Press.
- Karlsson, G. (1992). The grounding of psychological research in a phenomenological epistemology. *Theory & Psychology*, 2(4), 403-429.
doi:10.1177/0959354392024001
- Karlsson, G. (1993). *Psychological qualitative research from a phenomenological perspective*. Stockholm, Sweden: Almqvist & Wiskell International.
- Keen, E. A. (1975). *A primer in phenomenological psychology*. New York, NY: Holt, Reinhart, and Winston, Inc.
- Keen, P. G. W. (1981). Information systems and organizational change. *Communications of the ACM*, 24(1), 24-33. doi:10.1145/358527.358543
- Kehler, R. (2009, February 27). *Cyber war: The epitome of irregular warfare*. In *Cross Domain Integration: Warfare in the 21st Century*. Presented at the 25th Annual AFA Air Warfare Symposium and Technology Exposition, Orlando, FL.

- Keller, J. W., & Yang, Y. E. (2008). Leadership style, decision context, and the poliheuristic theory of decision-making: An experimental analysis. *Journal of Conflict Resolution*, 52(5), 687-712. doi:10.1177/0022002708320889
- Kelley, A. (2003). *Decision making using game theory: An introduction for managers*. New York, NY: Cambridge University Press.
- Kelly, J., & Kilcullen, D. (2006). Chaos versus predictability: A critique of effects-based operations. *Security Challenges*, 2(1), 63-73. Retrieved from <http://www.dtic.mil/dtic/>
- Kelsey, J. T. G. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review*, 106(7), 1427-1451. Retrieved from [http:// www.michiganlawreview.org/](http://www.michiganlawreview.org/)
- Kendall, J. (1999). Axial coding and the grounded theory controversy. *Western Journal of Nursing Research*, 21(6), 743-757. doi:10.1177/019394599902100603
- Kennedy, D. (2006). Computer networks, proportionality, and military operations. In A. M. Helm (Ed.), *The Law of War in the 21st Century: Weaponry and the Use of Force (International Law Studies, Volume 82, pp. 3-33)*. Newport, RI: Naval War College.
- Keyes, D. V., Simens, S. V., Kurtz, J. H., & York, S. T. (1997). Toward deterrence in the cyber dimension. *Report to the President's Commission on Critical Infrastructure Protection*. Retrieved from <http://www.dtic.mil/dtic/>
- Khalilzad, Z. (1999). Defense in a wired world: Protection, deterrence, prevention. In Z. Khalilzad, J. P. White & A. W. Marshall (Eds.), *Strategic Appraisal: The*

Changing Role of Information in Warfare (pp. 403-437). Santa Monica, CA: RAND Corporation.

Klein, G. A., Orasanu, J., Calderwood, R., & Zsombok, C. E. (1993). *Decision making in action: Models and methods*. Norwood, NJ: Ablex Publishing.

Kleindorfer, P. R. (2008, January 10). *Reflections on decision making under uncertainty*. In *Risk Management and Decision Processes*. Presented at the Known, the Unknown, and the Unknowable Conference, The Wharton School of the University of Pennsylvania, Philadelphia, PA.

Kleinrock, L. (1962). *Message delay in communication nets with storage* (Doctoral dissertation). Retrieved from <http://dspace.mit.edu/>

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management*, 23(2), 76-87. Retrieved from <http://www.ebscohost.com/>

Knight, F. H. (1921). *Risk, uncertainty, and profit*. Boston, MA: Houghton Mifflin Company.

Knight, J., Tulloch, D., & Knight, J. (2004). Does catastrophe theory represent a major development in mathematics? *Science in Dispute*, 3, 161-168. Retrieved from <http://www.gale.cengage.com/>

Korns, S. W., & Kastenber, J. E. (2008). Georgia's cyber left hook. *Parameters: US Army War College*, 38(4), 60-76. Retrieved from <http://www.ebscohost.com/>

Kornuta, H. M., & Germaine, R. W. (2006). *Research in education: A student and faculty guide to writing a research study*. Bloomington, IN: AuthorHouse.

Kramer, F. D., Starr, S. H., Wentz, L. K., Zimet, E., & Kuehl, D. T. (2007, June 19).

Frameworks and insights characterizing trends in cyberspace and cyberpower.

Presented at the 12th International Command and Control Research and

Technology Symposium - Adapting C2 to the 21st Century, Department of

Defense, Newport, RI.

Krulak, C. C. (1997, June 20). Warfighting. *Marine Corps Doctrinal Publication 1*.

Retrieved from <http://www.dtic.mil/dtic/>

Kuehl, D. T. (2002). Information operations, information warfare, and computer network

attack: Their relationship to national security in the information age. In M. N.

Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International*

Law (International Law Studies, Volume 76, pp. 35-58). Newport, RI: Naval War

College.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D.

Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp.

24-42). Washington, DC: Potomac Books, Inc.

Kugler, R. L. (2002, December). Dissuasion as a strategic concept. *Strategic Forum*, 196,

1-8. Retrieved from <http://www.dtic.mil/dtic/>

Kugler, R. L. (2009). Deterrence of cyber attacks. In F. D. Kramer, S. H. Starr & L. K.

Wentz (Eds.), *Cyberpower and National Security* (pp. 309-342). Washington, DC:

Potomac Books, Inc.

Kunsman, D. M., & Lawson, D. B. (2001, January). A primer on U.S. strategic nuclear

policy. *Sandia National Laboratory Report*. Retrieved from

<http://www.dtic.mil/dtic/>

- Kvale, S. (1996). *Interviews: An introduction to qualitative research interviewing*. Thousand Oaks, CA: Sage.
- Landauer, T. K., Foltz, P. W., & Laham, D. (1998a). An introduction to latent semantic analysis. *Discourse Processes*, 25(2/3), 259-284. Retrieved from <http://www.ebscohost.com/>
- Landauer, T. K., Foltz, P. W., & Laham, D. (1998b). The measurement of textual coherence with latent semantic analysis. *Discourse Processes*, 25(2/3), 285-307. Retrieved from <http://www.ebscohost.com/>
- Landler, M., & Markoff, J. (2007, May 29). Digital fears emerge after data siege in Estonia. *International Herald Tribune (Global Edition of the New York Times)*. Retrieved from <http://www.nytimes.com/>
- Langdridge, D. (2008). Phenomenology and critical social psychology: Directions and debates in theory and research. *Social and Personality Psychology Compass*, 2(3), 1126-1142. doi:10.1111/j.1751-9004.2008.00114.x
- Langfeldt, L. (2004). Judging quality - Expert panels evaluating research: Decision-making and sources of bias. *Research Evaluation*, 13(1), 51-62. doi:10.3152/147154404781776536
- Lanza, M. L. (2000). Nonlinear dynamics: Chaos and catastrophe theory. *Journal of Nursing Care Quality*, 15(1), 55-65. Retrieved from <http://www.proquest.com/>
- Laursen, J. V. (2007, December). *The history of the Internet*. Retrieved from <http://www.vissing.dk/inthist.html>
- Leavitt, H. J. (1965). Applied organizational change in industry. In J. G. March (Ed.), *Handbook of Organizations* (pp. 1144-1170). Chicago, IL: Rand McNally.

- Lee, L. S., & Fang, Y. S. (2009). A review and synthesis of recent research in Second Life. *Interactive Technology and Smart Education*, 6(4), 261-267.
doi:10.1108/17415650911009236
- Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly*, 22(4), 557-584.
doi: 10.1037/1045-3830.22.4.557
- Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). Upper Saddle River, NJ: Pearson.
- Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. S. (1997). The past and future history of the Internet. *Communications of the ACM*, 40(2), 102-108. doi:10.1145/253671.253741
- Leonard, R. J. (1995). From parlor games to social science: Von Neumann, Morgenstern, and the creation of game theory 1928-1944. *Journal of Economic Literature*, 33(2), 730-761. Retrieved from <http://www.ebscohost.com/>
- Levy, J. S. (1992). An introduction to prospect theory. *Political Psychology*, 13(2), 171-186. Retrieved from <http://www.jstor.org/>
- Lewis, J. A. (2002, December). *Assessing the risks of cyber terrorism, cyber war, and other cyber threats*. Retrieved from <http://www.dtic.mil/dtic/>
- Lewis, J. A. (2007, June 15). *Cyber attacks explained*. Retrieved from <http://www.dtic.mil/dtic/>
- Lewis, J. A., Langevin, J. R., McCaul, M. T. C. S., & Raduege, H. (2008, December). Securing cyberspace for the 44th Presidency. *Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Retrieved from <http://www.dtic.mil/dtic/>

- Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.
- Lichstein, H. (1963). Services curtailed: Telephone hackers active. *The Tech*, 83(24), 1-8.
Retrieved from <http://tech.mit.edu/V83/PDF/N24.pdf>
- Licklider, J. C. R. (1963, April 23). *Memorandum for members and affiliates of the intergalactic computer network*. Retrieved from <http://www.kurzweilai.net/>
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Newbury Park, CA: Sage Publications.
- Linstone, H. A., & Turoff, M. (1975). Introduction: General remarks. In H. A. Linstone & M. Turoff (Eds.), *The Delphi method: Techniques and applications* (pp. 3-12). Newark, NJ: New Jersey Institute of Technology.
- Liu, J. Y., Chen, H. G., Chen, C. C., & Sheu, T. S. (2010). Relationships among interpersonal conflict, requirements uncertainty, and software project performance. *International Journal of Project Management*. Advance online publication. doi:10.1016/j.ijproman.2010.04.007
- Livingston, S. (1997, June). Clarifying the CNN effect: An examination of media effects according to type of military intervention. In (John F. Kennedy School of Government, Ed.) *Research Paper R-18*.
- Loomes, G., & Sugden, R. (1982, December). Regret theory: An alternative theory or rational choice under uncertainty. *The Economic Journal*, 92, 805-824. Retrieved from <http://www.jstor.org/>
- Lorenz, E. N. (1963). Deterministic non-periodic flow. *Journal of the Atmospheric Sciences*, 20, 130-141. doi:10.1175/1520-0469(1963)020

- Lorenz, E. N. (1972, January 29). *Predictability: Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?* In AAAS Section on Environmental Sciences *New Approaches to Global Weather: The Global Atmospheric Research Program (GARP)*. Presented at the American Association for the Advancement of Science, 139th Meeting, Sheraton Park Hotel, Atlantic City, NJ.
- Luborsky, M. R., & Rubinstein, R. L. (1995). Sampling in qualitative research: Rationale, issues, and methods. *Research on Aging*, 17(1), 89-113.
doi:10.1177/0164027595171005
- Luce, R. D., & Raiffa, H. (1957). *Games and decisions: Introduction and critical survey*. New York, NY: Dover Publications, Inc.
- Macz, M. (2002). *Internet underground: The way of the hacker*. Otsego, MI: PageFree Publishing, Inc.
- Marill, T., & Roberts, L. G. (1966, November 7). *Toward a cooperative network of time-shared computers*. Presented at the AFIPS Joint Computer Conference, San Francisco, CA.
- Markoff, J. (2008, August 13). Before the gunfire, cyber attacks. *The New York Times*.
Retrieved from <http://www.nytimes.com/>
- Marshall, M. N. (1996a). Sampling for qualitative research. *Family Practice*, 13(6), 522-526. Retrieved from <http://www.oup.com/>
- Marshall, M. N. (1996b). The key informant technique. *Family Practice*, 13(10), 92-97.
Retrieved from <http://www.oup.com/>

- Marsico, E. M. (2010). Social networking websites: Are MySpace and Facebook the fingerprints of the twenty-first century? *Widener Law Journal*, 19(3), 967-976.
Retrieved from <http://www.ebscohost.com/>
- Mathers, R. F. (2007). *Cyberspace coercion in phase 0/1: How to deter armed conflict*. Newport, RI: Joint Military Operations Department, Naval War College.
- Matthews, W. (2008). Security experts: Cyber attacks will increase. *Air Force Times, Cyber Pro Newsletter*, 1(13), 1-21. Retrieved from <http://www.nsci-va.org/>
- Mazanec, B. M. (2009). The art of (cyber) war. *The Journal of International Security Affairs*, 16, 1-14. Retrieved from <http://www.securityaffairs.org/issues/2009/16/mazanec.php>
- McCauley-Bell, P., & Freeman, R. (1997). Uncertainty management in information warfare. In *1997 International Conference on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation* (Vol. 2, pp. 1942-1947). Orlando, FL: IEEE.
- McFedries, P. (2004, February). Hacking unplugged. *IEEE Spectrum*, 80. Retrieved from <http://ieeexplore.ieee.org/Xplore/>
- Meernik, J. (1994). Presidential decision making and the political use of military force. *International Studies Quarterly*, 38, 121-138. Retrieved from <http://www.jstor.org/>
- Melikishvili, A. (2008). The cyber dimension of Russia's attack on Georgia. *The Ukrainian Weekly*, 76(38), 1-2. Retrieved from <http://www.proquest.com/>

- Mertens, D. M. (2005). *Research and evaluation in education and psychology: Integrating, diversity with quantitative, qualitative, and mixed methods* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Micewski, E. R. (2003). Education of (military) leadership personnel in a postmodern world. *Defense Studies*, 3(3), 1-8. doi:10.1080/14702430308405074
- Michael, J. B., Wingfield, T. C., & Wijesekera, D. (2003, October 13). *Measured responses to cyber attacks using Schmitt analysis: A case study of attack scenarios for a software-intensive system*. Presented at the 27th Annual International Computer Software and Applications Conference, Dallas, TX: IEEE.
- Middleton, B. (1999). Using the hacker's toolbox. *Security Management Magazine*. Retrieved from <http://www.securitymanagement.com/library/000689.html>
- Miller, J. H. (2000). Information warfare: Issues and perspectives. In R. E. Neilson (Ed.), *Sun Tzu and information warfare* (pp. 145-167). Washington, DC: National Defense University.
- Mintz, A. (1993, December). The decision to attack Iraq: A noncompensatory theory to decision-making. *Journal of Conflict Resolution*, 37(4), 595-618. doi:10.1177/0022002793037004001
- Mintz, A. (1995). The 'noncompensatory principle' of coalition formation. *Journal of Theoretical Politics*, 7(3), 335-349. doi:10.1177/0951692895007003006
- Mintz, A. (2004). How do leaders make decisions? A poliheuristic perspective. *Journal of Conflict Resolution*, 48(1), 3-13. doi:10.1177/0022002703261056

- Mintz, A. (2005). Applied decision analysis: Utilizing poliheuristic theory to explain and predict foreign policy and national security decisions. *International Studies Perspectives*, 6, 94-98. doi:10.1111/j.1528-3577.2005.00195.x
- Mintz, A., Geva, N., & DeRouen, K. (1994). Mathematical models of foreign policy decision-making: Compensatory vs. noncompensatory. *Synthese*, 100(3), 441-460. doi:10.1007/BF01063911
- Mitroff, I. I., & Sagasti, F. (1973). Epistemology as general systems theory: An approach to the design of complex decision-making experiments. *Philosophy of the Social Sciences*, 3, 117-134. doi:10.1177/004839317300300109
- Moffat, J. (2003). Complexity theory and network centric warfare. *Information Age Transformation Series Report*. Retrieved from <http://www.dtic.mil/dtic/>
- Mongin, P. (1997). Expected utility theory. In J. Davis, W. Hands & U. Maki (Eds.), *Handbook of Economic Methodology* (pp. 342-350). London, United Kingdom: Edward Elgar Publishing.
- Morse, J. M. (1997). The pertinence of pilot studies. *Qualitative Health Research*, 7(3), 323-324. doi:10.1177/104973239700700301
- Moteff, J., & Parfomak, P. (2004, October 1). Critical infrastructure and key assets: Definition and identification. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>
- Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications.

- Murphy, B. M. (2001). *Mapping the pre-history of cyberspace and the making of social movement computer networks 1973-1993* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI Number: 3027234)
- Murray, P. J. (1998). Complexity theory and the fifth discipline. *Systemic Practice and Action Research*, 11(3), 275-293. doi:10.1023/A:1022900130219
- Murray, P. J. (2003). So what's new about complexity? *Systems Research and Behavioral Science*, 20, 409-417. doi:10.1002/sres.562
- Muto, S. A., & Martin, F. (2009). Portrait of Adrian van Kaam and humanistic psychology. *Journal of Humanistic Psychology*, 49(3), 355-375.
doi:10.1177/0022167809333998
- Myers, R. B. (2004). *The national military strategy of the United States of America*. Retrieved from <http://www.dtic.mil/dtic/>
- Nadler, D. A., & Tushman, M. L. (1980). A model for diagnosing organizational behavior. *Organizational Dynamics*, 9(2), 35-51. Retrieved from <http://www.elsevier.com/>
- Napolitano, J. (2010, February 1). *Quadrennial security review report: A strategic framework for a secure homeland*. Retrieved from <http://www.dtic.mil/dtic/>
- Nash, J. (1950). The bargaining problem. *Econometrica*, 18(2), 155-162. Retrieved from <http://www.ebscohost.com/>
- Nash, J. (1953). Two-person cooperative games. *Econometrica*, 21(10), 128-140.
Retrieved from <http://www.ebscohost.com/>
- National Security Council. (2010). *National Security Council*. Retrieved from <http://www.whitehouse.gov/administration/eop/nsc/>

- Neary, T., Preisinger, J., Ludka, L., & Sutter, J. (2001, January 21). A baseline assessment of DoD staff nuclear expertise: Final report. In (Defense Threat Reduction Agency, Ed.) *Nuclear Deterrence Issues and Options Study. Advance Systems and Concepts Office, SAIC Strategies Group*. Retrieved from <http://www.dtic.mil/dtic/>
- Nelson, R. (1987). Stochastic catastrophe theory in computer performance modeling. *Journal of the Association for Computing Machinery*, 34(3), 661-685. doi:10.1145/28869.28878
- Neuman, W. L. (2003). *Social research methods: Qualitative and quantitative approaches* (5th ed.). Boston, MA: Allyn and Bacon.
- Neumann, P. G. (1995). *Computer-related risks*. New York, NY: Addison-Wesley Publishing Company.
- Nguyen, N., Reiher, P., & Kuenning, G. H. (2003). *Detecting insider threats by monitoring system call activity*. Presented at the Proceedings of the 2003 IEEE Workshop on Information Assurance, West Point, NY: IEEE Xplore.
- Nicholson, D. J. (2005). "Seeing the other side of the hill:" The art of battle command, decision-making, uncertainty, and the information superiority complex. *Military Review*, 85(6), 57-64. Retrieved from <http://www.ebscohost.com/>
- Nincic, M. (1997). Loss aversion and the domestic context of military intervention. *Political Research Quarterly*, 50(1), 97-120. doi:10.1177/106591299705000105
- Nissenbaum, H. (1998, March). Values in the design of computer systems. *Computer in Society*, 38-39. Retrieved from <http://portal.acm.org/>

- Nizza, M. (2008, August 11). Georgia's leader, under siege online and off. *The New York Times (The Lede)*. Retrieved from <http://thelede.blogs.nytimes.com>
- North Atlantic Treaty. (1949, April 4). *The North Atlantic treaty*. Retrieved from <http://www.nato.int/docu/basic/txt/treaty.htm>
- Nunes, P. F. V. (1999, September 13). *The impact of new technologies in military arena: Information warfare*. Presented at the International Congress of Military Press, Lisbon, Portugal: Revista Militar.
- Obama, B. H. (2009, June). *Cyberspace policy review: Assuring a trusted and resilient information and communication infrastructure*. Retrieved from <http://www.whitehouse.gov/assets/documents/>
- Obama, B. H. (2010, May). *National security strategy*. Retrieved from <http://www.whitehouse.gov/sites/default/files/>
- O'Donnell, B. T., & Kraska, J. C. (2002). International law of armed conflict and computer network attack: Developing the rules of engagement. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76, pp. 395-420)*. Newport, RI: Naval War College.
- Oros, C. J., Doan, H. M., Adoum, D. D., & MacDonald R. C. (2007). Portfolio review expert panel (PREP) process: A tool for accountability and strategic planning to meet research goals. *Research Evaluation*, 16(3), 157-167.
doi:10.3152/095820207X239436
- Orwell, G. (1945, October 19). You and the atomic bomb. *Tribune*. Retrieved from <http://www.tribunemagazine.co.uk/>

- Ospina, S. (2004). Qualitative research. In G. R. Goethals, G. J. Sorenson & J. M. Burns (Eds.), *Encyclopedia of Leadership* (pp. 1279-1284). Thousand Oaks, CA: Sage Publications.
- Ostrom, C., & Job, B. (1986). The president and the political use of force. *American Political Science Review*, 80, 541-566. Retrieved from <http://www.jstor.org/>
- Owen, R. S. (2008). Infrastructures of cyber warfare. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber warfare and cyber terrorism* (pp. 35-41). Hershey, PA: Information Science Reference.
- Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyber attack capabilities*. Washington, DC: The National Academies Press.
- Pace, P. (2006a, December). *The national military strategy for cyberspace operations*. Retrieved from <http://www.dtic.mil/dtic/>
- Pace, P. (2006b, September 17). *Joint operations*. Retrieved from <http://www.dtic.mil/dtic/>
- Paparone, C. R. (2001). U.S. Army decision-making: Past, present, and future. *Military Review*, 81(4), 45-53. Retrieved from <http://www.ebscohost.com/>
- Papp, D. S., & Alberts, D. S. (1997). Technology and change in human affairs. In D. S. Alberts & D. S. Papp (Eds.), *The information age: An anthology on its impact and consequences* (pp. ii-viii). Washington, DC: CCRP Publication Series. Retrieved from <http://www.dodccrp.org/>
- Patton, M. Q. (2002). *Qualitative evaluation and research methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.

- Peng, L., Wijesekera, D., Wingfield, T. C., & Michael, J. B. (2006). An ontology-based distributed whiteboard to determine legal responses to online cyber attacks. *Internet Research*, 16(5), 475-490. doi:10.1108/10662240610710969
- Peng, L., Wingfield, T., Wijesekera, D., Frye, E., Jackson, R., & Michael, J. (2006). Making decisions about legal responses to cyber attacks. In International Federation for Information Processing (Ed.), *Advances in Digital Forensics* (pp. 283-294). Boston, MA: SpringerLink.
- Peppler, C. (2007, June 22). *Pentagon cyber attack forces 1,500 PCs off line*. Retrieved from <http://www.foxnews.com/>
- Perine, K. (2000, October 23). The early adopter: Al Gore and the Internet - Government activity. *The Industry Standard*. Retrieved from http://findarticles.com/p/articles/mi_m0HWW/is_43_3/ai_66672985/
- Pfister, H. R., & Böhm, G. (2008). The multiplicity of emotions: A framework of emotional functions in decision making. *Judgment and Decision Making*, 3(1), 5-17. Retrieved from <http://www.ebscohost.com/>
- Phillips, M. (2007). Uncertain justice for nuclear terror: Deterrence of anonymous attacks through attribution. *Orbis*, 51(3), 429-446. doi:10.1016/j.orbis.2007.04.005
- Phister, P. W., Fayette, D., & Krzysiak, E. (2005, March 28). CyberCraft: Concept linking network-centric warfare principles with the cyber domain in an urban operational environment. *Effects Based Operations Report*. Retrieved from <http://www.dtic.mil/dtic/>
- Pinch, T. J., & Bijker, W. E. (1987). The social construction of facts and artifacts: Or how sociology of science and the sociology of technology might benefit from

- each other. In W. E. Bijker, T. P. Hughes & T. Pinch (Eds.), *The Social Construction of Technological Systems* (pp. 17-50). Cambridge, MA: MIT Press.
- Poincaré, J. H. (1890). Sur le problème des trois corps et les équations de la dynamique: Divergence des séries de M. Lindstedt. *Acta Mathematica*, 13, 1-270.
- Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology*, 52(2), 137-145. Retrieved from <http://www.ebscohost.com/>
- Post, J. V. (1979). Cybernetic war. In O. Davies (Ed.), *The Omni Book of Computers & Robots* (pp. 343-358). New York, NY: Kensington Publishing Corporation.
- Power, M. (2007). Digitized virtuosity: Video war games and post-9/11 cyber-deterrence. *Security Dialogue*, 38(2), 271-288. doi:10.1177/0967010607078552
- Priest, H. (2002). An approach to the phenomenological analysis of data. *Nurse Researcher*, 10(2), 50-63. Retrieved from <http://www.proquest.com/>
- QSR International. (2007). *Qualitative research*. Retrieved from <http://www.qsrinternational.com/>
- Qvortrup, L. (2006). Understanding new digital media: Medium theory or complexity theory? *European Journal of Communication*, 21(3), 345-356. doi:10.1177/0267323106066639
- Radnor, Z. J. (1999). *Lean working practices: The effect on the organization*. Manchester, England: Manchester School of Management.
- Radnor, Z. J., & Boadan, R. (2004). Developing an understanding of corporate anorexia. *International Journal of Operations & Production Management*, 24(4), 424-440. doi:10.1108/01443570410524677

- Ramirez, C. (2002, November 15). *Strategies for subject matter expert review in questionnaire design*. Presented at the Questionnaire Design, Evaluation, and Testing Conference, Charleston, SC.
- Rattray, G. J. (2001). *Strategic warfare in cyberspace*. Cambridge, MA: MIT Press.
- Redd, S. B. (2002). The influence of advisers on foreign policy decision making: An experimental study. *Journal of Conflict Resolution*, 46(3), 335-364.
doi:10.1177/0022002702046003002
- Reed, W., Clark, D. H., Nordstrom, T., & Hwang, W. (2008). War, power, and bargaining. *The Journal of Politics*, 70, 1203-1216.
doi:10.1017/S0022381608081152
- Reid, T. (2007, September 8). *China's cyber army is preparing to march on America, says Pentagon*. Retrieved from <http://www.timesonline.com/>
- Report to Congress. (2007, November). U.S. - China economic and security review commission. In (Bartholomew, C., & Blumenthal, D. A., Eds.) *One Hundred Tenth Congress - First Session*. Retrieved from <http://www.uscc.gov>
- Rhodin, S. (2008, July 1). Hackers tag Lithuanian web sites with Soviet symbols. *The New York Times*. Retrieved from <http://www.nytimes.com/>
- Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, 4, 155-169. doi:10.1007/BF01405730
- Roberts, A. S., Hopp, T., Sorensen, E. W., Benrimoj, S. I., Chen, T. F., Herborg, H., . . . Aslani, P. (2003). Understanding practice change in community pharmacy: A qualitative research instrument based on organizational theory. *Pharmacy World & Science*, 25(5), 227-234. doi:10.1023/A:1025880012757

- Robertson Jr., H. B. (2002). Self-defense against computer network attack under international law. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76*, pp. 121-146). Newport, RI: Naval War College.
- Robson, C. (2002). *Real world research: A resource for social scientists and practitioner-researchers* (2nd ed.). Malden, MA: Wiley-Blackwell.
- Rogers, J. (2008, January 17). U.S. in middle of cyber war with China, Russia? *SC Magazine*. Retrieved <http://www.scmagazineus.com>
- Roman, P. J., & Tarr, D. W. (1998). The Joint Chiefs of Staff: From service parochialism to jointness. *Political Science Quarterly*, 113(1), 91-111. Retrieved from <http://www.ebscohost.com/>
- Rona, T. P. (1976, July). *Weapon systems and information war*. Research Report, Boeing Aerospace Company, Seattle, WA.
- Rosenbach, E., & Klajn, T. (2008, July 18). China's cyber warriors (Belfer Center for Science and International Affairs, Ed.). *Baltimore Sun*. Retrieved from http://belfercenter.ksg.harvard.edu/publication/18440/chinas_cyber_warriors.html
- Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting*, 15(4), 353-375.
doi:10.1016/S0169-2070(99)00018-7
- Rowe, N. C. (2007). Ethics of cyber war attacks. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 105-111). Hershey, PA: Information Science Reference.

- Royakkers, L., & van Est, R. (2010). The cubicle warrior: The marionette of digitalized warfare. *Ethics and Information Technology*, 12(3), 289-296.
doi:10.1007/s10676-010-9240-8
- Rumsfeld, D. H. (2005, March). *The national defense strategy*. Retrieved from <http://www.dtic.mil/dtic/>
- Saunders, T. F., & Levis, A. H. (2007, August). Report on implications of cyber warfare. *United States Air Force Scientific Advisory Board Final Report: Volumes 1 and 2*. Retrieved from <http://www.dtic.mil/dtic/>
- Schechtman, G. M. (1996). *Manipulating the OODA loop: The overlooked role of information resource management in information warfare* (Unpublished doctoral dissertation). Air Force Institute of Technology, Air University, Logistics and Acquisition Management, Wright-Patterson Air Force Base, OH.
- Schell, B. H., & Martin, C. (2004). *Cybercrime: A reference handbook*. Santa Barbara, CA: ABC-CLIO.
- Schell, W. J., Youngblood, A. D., & Farrington, P. A. (2008, May 17). *An investigation into the antecedent experiences of transformational leaders: Research approach and initial findings*. Presented at the 2008 Industrial Engineering Research Conference, Vancouver, British Columbia, Canada.
- Schelling, T. C. (1956). An essay on bargaining. *The American Economic Review*, 46(3), 281-306. Retrieved from <http://www.ebscohost.com/>
- Schelling, T. C. (1957). Bargaining, communication, and limited war. *Journal of Conflict Resolution*, 1(19), 19-36. doi:10.1177/002200275700100104
- Schelling, T. C. (1960). *The strategy of conflict*. Cambridge, MA: Harvard University.

- Schelling, T. C. (1966). *Arms and influence*. New Haven, CT: Yale University Press.
- Schelling, T. C. (2005). Reciprocal measures for arms stabilization. *Daedalus*, 134(4), 101-117. doi:10.1080/00396336108440237
- Schlesinger, J. R. (1976). The evolution of American policy towards the Soviet Union. *International Security*, 1(1), 37-48. Retrieved from <http://www.ebscohost.com/>
- Schlesinger, J. R. (1993). The impact of nuclear weapons on history. *The Washington Quarterly*, 16(4), 5-12. Retrieved from <http://www.gale.cengage.com/>
- Schmitt, J. F. (1997). Command and (out of) control: The military implications of complexity theory. In D. S. Alberts & T. J. Czerwinski (Eds.), *Complexity, global politics, and national security* (pp. 99-111). Washington, DC: National Defense University.
- Schmitt, M. N. (1998). Bellum Americanum: The U.S. view of twenty-first century war and its possible implications for the law of armed conflict. *Michigan Journal of International Law*, 19, 1051-1090. Retrieved from <http://support.lexisnexis.com/>
- Schmitt, M. N. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *The Columbia Journal of Transnational Law*, 37, 885-937. Retrieved from <http://www.dtic.mil/dtic/>
- Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *IRRC*, 84(846), 365-399. Retrieved from <http://online.sagepub.com/>
- Schmitt, M. N. (2006). War, technology, and the law of armed conflict. In A. M. Helm (Ed.), *The Law of War in the 21st Century: Weaponry and the Use of Force* (*International Law Studies, Volume 82*, pp. 137-182). Newport, RI: Naval War College.

- Schneider, J. J. (1997, Spring). Black lights: Chaos, complexity, and the promise of information warfare. *Joint Force Quarterly*, 15, 21-28. Retrieved from <http://www.dtic.mil/dtic/>
- Schneidewind, N. F. (2008). Cyber security models. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 228-240). Hershey, PA: Information Science Reference.
- Schramm, W. (1971). *Notes on case studies*. Retrieved from <http://029c7c0.netsolhost.com/publications.html>
- Schultz, E. E. (2002, October 30). *A framework for understanding and predicting insider attacks*. Presented at the Compsec 2002, London, United Kingdom: Elsevier Science Ltd.
- Schultz, J. V. (1997). *A framework for military decision making under risks* (Unpublished doctoral dissertation). Air Force Institute of Technology, Air University, School of Advanced Airpower Studies, Wright-Patterson Air Force Base, OH.
- Schutz, A. (1967). *The phenomenology of the social world*. Evanston, IL: Northwestern University Press.
- Schwandt, T. A. (2002). *Dictionary of qualitative perspective* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Scott, B. D. (2008). Governments, civilians, and the evolution of insurgency: Modeling the early dynamics of insurgencies. *Journal of Artificial Societies & Social Simulation*, 11(4), 11-17. Retrieved from <http://www.ebscohost.com/>

- Seidman, I. E. (2006). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (3rd ed.). New York, NY: Teachers College Press.
- Shachtman, N. (2008, August 11). Estonia, Google help 'cyberlocked' Georgia. *Wired Magazine*. Retrieved from <http://blog.wired.com/defense/2008/08/civilge-the-geo.html>
- Shao, W., Lye, A., Rundle-Thiele, S., & Fausnaugh, C. (2003). Decision theory: Poised for the new millennium. In *ANZMAC 2003 Adelaide Conference Proceedings* (pp. 670-685). Australian & New Zealand Marketing Academy.
- Sharma, S. K., & Gupta, J. N. D. (2002). Securing information infrastructure from information warfare. *Logistics Information Management*, 15(5/6), 414-422. doi:10.1108/09576050210447118
- Sharp, Sr., W. G. (1999a). *Cyberspace and the use of force*. Falls Church, VA: Aegis Research Corporation.
- Sharp, Sr., W. G. (1999b). Balancing our civil liberties with our national security interests in cyberspace. *Texas Review of Law & Politics*, 4(1), 69-75. Retrieved from <http://www.ebscohost.com/>
- Sharp, W. G. (2008). *Democracy and deterrence: Foundations for an enduring world peace*. Maxwell Air Force Base, AL: Air University Press.
- Sharp, W. L. (2006, February 13). Information operations. *Joint Publication 3-13*. Retrieved from <http://www.dtic.mil/dtic/>
- Shea, D. A. (2003, July 14). Critical infrastructure: Control systems and the terrorist threat. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>

- Shelton, H. H. (1998, October 9). Joint doctrine for information operations. *Joint Publication 3-13*. Retrieved from <http://www.dtic.mil/dtic/>
- Shelton, H. H. (2000, January 15). Standing rules of engagement for US forces. *Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01A*. Retrieved from <http://www.dtic.mil/dtic/>
- Shen, D., Chen, G., Cruz, J. B., Blasch, E., & Kruger, M. (2007, June 19). *Game theoretic solutions to cyber attack and network defense problems*. In *C2 Concepts, Theory, and Policy*. Presented at the 12th International Command and Control Research and Technology Symposium - Adapting C2 to the 21st Century, Newport, RI.
- Silver, D. B. (2002). Computer network attack as a use of force under Article 2(4) of the United Nations Charter. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76*, pp. 73-98). Newport, RI: Naval War College.
- Simon, H. A. (1955). A behavioral model of rational choice. *Quarterly Journal of Economics*, 69(1), 99-118. Retrieved from <http://www.ebscohost.com/>
- Simon, H. A. (1959). Theories of decision-making in economics and behavioral science. *The American Economic Review*, 49(3), 253-283. Retrieved from <http://www.ebscohost.com/>
- Simpkin, R. (1987). *Deep battle: The brainchild of Marshal Tukhachevskii*. London, United Kingdom: Brassey's Defense Publishers.
- Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. New York, NY: The Penguin Press.

- Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977). Behavioral decision theory. *Annual Review of Psychology*, 28, 1-39. doi:10.1146/annurev.ps.28.020177.000245
- Smith, C., Norton, B., & Ellis, D. (1992). Leavitt's diamond and the flatter library. *Library Management*, 13(5), 18-22. doi:10.1108/01435129210020352
- Smith, E. A. (2003). *Effects based operations: Applying network centric warfare in peace, crisis, and war*. Retrieved from http://www.dodccrp.org/files/Smith_EBO.pdf
- Smith, E. A. (2006, July). Complexity, networking, & effects-based approaches to operations. *Command and Control Research Program Report*. Retrieved from http://www.dodccrp.org/files/Smith_Complexity.pdf
- Smith, E. A. (2009, June 15). *Wicked problems and comprehensive thinking in irregular warfare*. In *C2 and Agility*. Presented at the 14th International Command and Control Research and Technology Symposium (ICCRTS), Washington, DC.
- Smith, J. K. (1983). Quantitative versus qualitative research: An attempt to clarify the issue. *Educational Researcher*, 12, 6-13. doi:10.3102/0013189X012003006
- Stake, R. E. (1995). *The art of case study research*. Thousand Oaks, CA: Sage Publications.
- Stake, R. E. (2000). Case studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 435-454). Thousand Oaks, CA: Sage Publications.
- Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2004, July 12). Analysis of end user security behaviors. *Computers & Security*, 1-10. doi:10.1016/j.cose.2004.07.001

- Starks, H., & Trinidad, S. B. (2007). Choose your method: A comparison of phenomenology, discourse analysis, and grounded theory. *Qualitative Health Research*, 17(10), 1372-1380. doi:10.1177/1049732307307031
- Starr, B. (1999, March 5). Pentagon cyberwar attack mounted through Russia. *Report of Cyber warfare: Foreign government hackers may be getting help from within the U.S. government*. Retrieved from <http://www.geocities.com/Area51/Shadowlands/6583/project399.html>
- Steinbruner, J. D. (1974). *The cybernetic theory of decision: New dimensions of political analysis*. Princeton, NJ: Princeton University Press.
- Stohl, M. (2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point, or patriot games? *Crime, Law, and Social Change*, 46(4-5), 223-238. doi:10.1007/s10611-007-9061-9
- Stoops, N. (2004). *Educational attainment in the United States: 2003* (U.S. Department of Commerce, Ed.). Retrieved from <http://www.census.gov/prod/2004pubs/p20-550.pdf>
- Stratfor. (2008a, April 16). *Cyber warfare 101: Black hats, white hats, crackers, and bots*. Retrieved from <http://www.stratfor.com/analysis/>
- Stratfor. (2008b, March 1). *Cyber warfare: A glossary of useful terms*. Retrieved from <http://www.stratfor.com/analysis/>
- Strauss, A. C., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques* (2nd ed.). Thousand Oaks, CA: Sage Publications.

- Strauss, A. C., & Corbin, J. (1994). Grounded theory methodology: An overview. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 273-285). Thousand Oaks, CA: Sage.
- Studer, J. (2005). *Are there five rings or a loop in fourth generation warfare? A study on the application of Warden's or Boyd's theories in 4GW* (Unpublished doctoral dissertation). Air University, Air Command and Staff College, Maxwell Air Force Base, AL.
- Suh, N. P. (1999). A theory of complexity, periodicity, and design axioms. *Research in Engineering Design*, 11, 116-131. doi:10.1007/PL00003883
- Suh, N. P. (2005). *Complexity: Theory and applications*. New York, NY: Oxford University Press.
- Svensson, P. (2008, August 11). Georgian president's website moves to Atlanta. *USA Today*. Retrieved from <http://www.usatoday.com/>
- Sylvan, D., & Majeski, S. (2006, March 22). *Reviving the cybernetic approach to foreign policy analysis: Explaining the continuity of U.S. policy instruments*. Presented at the 47th Annual Convention of the International Studies Association, San Diego, CA.
- Syvyanter, D. J., Deshon, R. P., & Siler, M. T. (1991). The illusion of certainty: A catastrophe model of decision framing. *Current Psychology*, 10(3), 199-209. doi:10.1007/BF02686775
- Taipale, K. A. (2009, March). Cyber deterrence (comment draft). In (IGI Global 2010, Ed.) *Law, policy, and technology: Cyberterrorism, information warfare, digital and Internet immobilization*. Retrieved from <http://www.global-info-society.org/>

- Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. New York, NY: Random House.
- Tenet, G. J. (2001, February 7). Computer network operations: A critical element of current and future military operations in combating the asymmetrical threat. *Report of Space, Missile Defense and Computer Network Operations Challenges*. Retrieved from <http://www.dtic.mil/dtic/>
- Tesch, R. (1980). *Phenomenological and transformative research: What they are and how to do them*. Santa Barbara, CA: Fielding Institute.
- The American Heritage Dictionary of the English Language* (4th ed.). (2006). Houghton Mifflin Company. Retrieved from <http://dictionary.reference.com/browse/decision>
- Thiéart, R. A., & Forgues, B. (1995). Chaos theory and organization. *Organization Science*, 6(1), 19-31. doi:10.1287/orsc.6.1.19
- Thirtle, M. R. (2001). *Educational benefits and officer-commissioning opportunities available to U.S. military service members* (RAND, Ed., pp. 1-110). Retrieved from <http://www.dtic.mil/dtic/>
- Thom, R. (1972). *Structural stability and morphogenesis: An outline of a general theory of models* (D. H. Fowler, Trans., English translation). W. A. Benjamin: New York, NY.
- Thomas, T. L. (2006, Summer). Cyber mobilization: A growing counterinsurgency campaign. *IOSphere*, 23-28. Retrieved from <http://www.dtic.mil/dtic/>
- Tikk, E., Kaska, K., Rünneri, K., Kert, M., Taliarm, A. M., & Vihul, L. (2008, August). Cyber attacks against Georgia: Legal lessons learned. *NATO*

- Cooperative Cyber Defense Center of Excellence Report*. Retrieved from <http://www.dtic.mil/dtic/>
- Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>
- Tubbs, D., Luzwick, P. G., & Sharp, W. G. (2002). Technology and law: The evolution of digital warfare. In M. N. Schmitt & B. T. O'Donnell (Eds.), *Computer Network Attack and International Law (International Law Studies, Volume 76*, pp. 7-20). Newport, RI: Naval War College.
- Turkle, S. (1984). *The second self: Computers and the human spirit*. New York, NY: Simon & Schuster, Inc.
- Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York, NY: Simon & Schuster, Inc.
- Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124-1131. Retrieved from <http://www.jstor.org/>
- Tzu, S. (1910). *The art of war* (L. Giles, Trans.). London, United Kingdom: Luzac & Co. (Original work published n.d.)
- U.S. Army Field Manual (FM) 3-0. (2008, February 27). *Operations*. Retrieved from <http://www.dtic.mil/dtic/>
- U.S. Army Field Manual (FM) 5-0. (2005, January 1). *Army planning and orders production*. Retrieved from <http://www.dtic.mil/dtic/>
- Vamosi, R. (2007, May 29). Cyber attack in Estonia: What it really means. *Newsmaker*. Retrieved from http://news.cnet.com/When-cyberattacks-are-politically-motivated/2008-7349_3-6186751.html

- van Kaam, A. L. (1959). Phenomenal analysis: Exemplified by a study of the experience of "feeling really understood." *Journal of Individual Psychology*, 15, 66-72.
- van Kaam, A. L. (1966). *Existential foundations of psychology*. New York, NY: Doubleday.
- van Kaam, A. L. (1972). *On being yourself: Reflections on spirituality and originality*. Rockaway, NJ: Dimension Books.
- Van Maanen, J. (1988). *Tales of the field: On writing ethnography*. Chicago, IL: The University Chicago Press.
- van Manen, M. (1990). *Researching lived experiences: Human science for an action sensitive pedagogy*. Albany, NY: State University of New York Press.
- Vandenberg, H. S. (1949, August). Investigation of the B-36 bomber program. *Military Establishment Appropriation Bill for 1948*. Retrieved from <http://www.dtic.mil/dtic/>
- von Neumann, J. (1928). Zur theorie der gesellschaftsspiele. *Mathematische Annalen*, 100, 295-320 (S. Bargmann, Trans.). In A. W. Tucker & R. D. Luce (Eds.), *Contributions to the Theory of Games. Vol. IV: Annals of Mathematics Studies* (40, pp. 13-42). Princeton, NJ: Princeton University Press.
- von Neumann, J., & Morgenstern, O. (1944). *Theory of games and economic behavior*. Princeton, NJ: Princeton University Press.
- Vowell, J. B. (2004). *Between discipline and intuition: The military decision making process in the Army's future force*. Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College.

- Wade, L. (2003). Terrorism and the Internet: Resistance in the information age. *Knowledge, Technology, & Policy*, 16(10), 104-127. doi:10.1007/s12130-003-1018-4
- Wallenius, K. (2005). *Generic support for decision-making in effects-based management of operations*. Kungliga Tekniska Hogskolan School of Computer Science and Communication, University of Stockholm, Sweden. (ISBN 91-7178-234-6)
- Warden, J. A. (1994). Air theory for the twenty-first century. In K. P. Magyar (Ed.), *Challenge and Response: Anticipating U.S. Military Security Concerns* (pp. 311-332). Maxwell Air Force Base, AL: Air University Press.
- Warren, C. A. B. (2001). Qualitative interviewing. In J. F. Gubrium & J. A. Holstein (Eds.), *Handbook of Interview Research: Context & Method* (pp. 83-101). Thousand Oaks, CA: Sage Publications.
- Waterman, P. A. (1997). *Resource evaluation and presidential decision-making: Predicting the use of force by U.S. Presidents, 1976-1988* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI Number: 1384462)
- Waters, G., Ball, D., & Dudgeon, I. (2008). *Australia and cyber warfare*. Canberra, Australia: Australian National University E Press.
- Webster, A. A. (2010). *Leveraging cyberspace in counterinsurgency operations* (Master's thesis). U.S. Army War College, Carlisle Barracks, PA.
- Wegener, H., Barletta, W. A., Bosch, O., Chereskin, D., Kamal, A., Krutskikh, A., . . . Westby, J. R. (2003, November 21). *Toward a universal order of cyberspace: Managing threats from cybercrime to cyberwar*. Presented at the International

Centre for Scientific Culture conducted at the World Summit on the Information Society, World Federal of Scientists Permanent Monitoring Panel on Information Security, Geneva, Switzerland.

Welch, L. D. (2007, November 1). Cyber deterrence and national security. In T. Fuhrman (Chair), *Keynote Address*. Cyber Deterrence, Booz Allen Hamilton, Tysons Corner, VA.

Wheeler, D. A., & Larsen, G. N. (2007, June 5). Techniques for cyber attack attribution. *Institute for Defense Analyses*. Retrieved from <http://www.dtic.mil/dtic/>

Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine*. Cambridge, MA: MIT Press.

Wilding, C., & Whiteford, G. (2005). Phenomenological research: An exploration of conceptual, theoretical, and practical issues. *OTJR: Occupation, Participation & Health*, 25(3), 98-104. Retrieved from <http://www.ebscohost.com/>

Willemsen, J. C. (2000, June 22). Critical infrastructure protection: Comments on the proposed cyber security information act of 2000. *United States General Accounting Office*. Retrieved from <http://www.dtic.mil/dtic/>

Wilson, C. (2003, October 17). Computer attack and cyber terrorism: Vulnerabilities and policy issues for congress. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>

Wilson, C. (2007a, November 15). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>

- Wilson, C. (2007b, June 5). Information operations, electronic warfare, and cyberwar: Capabilities and related policy issues. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>
- Wilson, C. (2008, January 29). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. *CRS Report for Congress*. Retrieved from <http://www.dtic.mil/dtic/>
- Wimpenny, P., & Gass, J. (2000). Interviewing in phenomenology and grounded theory: Is there a difference? *Journal of Advanced Nursing*, 31(6), 1485-1492.
doi:10.1046/j.1365-2648.2000.01431.x
- Wingfield, T. C. (2006, February). When is a cyber attack an “armed attack?” - Legal thresholds for distinguishing military activities in cyberspace. *The Potomac Institute for Policy Studies*. Retrieved from <http://www.dtic.mil/dtic/>
- Wingfield, T. C. (2007, August 21). Information operations in future wars. In *Chapters 6 and 7: The law of information conflict: National security law in cyberspace*. Aegis Research Corporation. Retrieved from <http://www.dtic.mil/dtic/>
- Wingfield, T. C. (2009). International law and information operations. In F. D. Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 525-543). Washington, DC: Potomac Books, Inc.
- Wingfield, T. C., & Michael, J. B. (2004, April 28). An introduction to legal aspects of operations in cyberspace. *Naval Postgraduate School*. Retrieved from <http://www.dtic.mil/dtic/>
- Wingfield, T. C., Michael, J. B., & Wijesekera, D. (2005, March 15). *Optimizing lawful responses to cyber intrusions*. Retrieved from <http://www.dtic.mil/dtic/>

- Wolcott, H. F. (1994). *Transforming qualitative data: Description, analysis, and interpretation*. Thousand Oaks, CA: Sage Publications.
- Wolk, H. S. (1976, July-August). Strategic deterrence: The fragile balance. *Air University Review*. Retrieved from <http://www.airpower.au.af.mil/>
- Wortzel, L. M. (2008, January 29). Enforcement of federal espionage laws. *Subcommittee on Crime and Homeland Security (Chair), House Committee on the Judiciary Report*, Washington, DC.
- Wright, L. (2008). The spymaster. *The New Yorker*, 83(44), 42-59. Retrieved from <http://www.ebscohost.com/>
- Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Thousand Oaks, CA: Sage Publications.
- Yukl, G. (1989). Managerial leadership: A review of theory and research. *Journal of Management*, 15(2), 251-289. doi:10.1177/014920638901500207
- Zeelenberg, M. (1999). Anticipated regret, expected feedback, and behavioral decision-making. *Journal of Behavioral Decision Making*, 12(2), 93-106.
doi:10.1002/(SICI)1099-0771(199906)12:2<93::AID-BDM311>3.0.CO;2-S
- Zimet, E., & Skoudis, E. (2009). A graphical introduction to the structural elements of cyberspace. In F. D. Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 91-112). Washington, DC: Potomac Books, Inc.
- Zsombok, C. E., & Klein, G. A. (1997). *Naturalistic decision making*. Mahwah, NJ: Lawrence Erlbaum Associates.

Appendix A: Review of the Literature Key Search Terms

Review of the Literature Key Search Terms

The following key terms and phrases were used for conducting the review of the literature:

Armed Attack

Chaos

Complexity

Computer Network Attack (CNA)

Computer Network Defense (CND)

Computer Network Exploitation (CNE)

Computer Network Operations (CNO)

Continuity of Operations Plan (COOP)

Counterintelligence (CI)

Critical Infrastructure

Cyber Attack

Cyber Crime

Cyber Terrorism

Cyber Warfare

Cyberspace

Cyberspace Operations

Decision-Making

Decision Theory

Defense Industrial Base (DIB)

Deterrence Theory

Effects-based Operations (EBO)

Electromagnetic Spectrum

Elements of National Power

Global Information Grid (GIG)

Hostile Act and Hostile Intent

Information Assurance (IA)

Information Environment

Information Operations (IO)

Information Warfare (IW)

Inherent Right of Self Defense

Intelligence

Internet

Jus in Bello (Latin)

Jus ad Bellum (Latin)

Law of Armed Conflict (LOAC)

Law of Information Conflict (LOIC)

Network Operations

Operational Preparation of the Environment (OPE)

Risk

Standing Rules of Engagement (SROE)

Strategic Communications (SC)

Threat

Uncertainty

Use of Force

Vulnerability

World Wide Web (WWW)

Appendix B: Computer Network Attack Methods

Computer Network Attack Tools and Techniques

Tool or Mode	Misuse Type or Technique
External	
Visual spying	Observing of keystrokes or screens
Misrepresentation	Deceiving operators and users
Physical scavenging	Dumpster-diving for printout
Hardware Misuse	
Logical scavenging	Examining discarded/stolen media
Eavesdropping	Intercepting electronic or other data
Interference	Jamming, electronic or otherwise
Physical attack	Damaging or modifying equipment, power, or media
Physical removal	Removing equipment and storage media
Masquerading	
Impersonation	Using false identities external to computer systems
Piggybacking attacks	Usurping communication lines, workstations
Spoofing attacks	Using playback, creating bogus nodes and systems
Network weaving	Masking physical whereabouts or routing
Pest Programs	Setting up opportunities for further misuse
Trojan horse attacks	Implanting malicious code, sending letter bombs
Logic bombs	Setting time or event bombs (a form of Trojan horse)
Malevolent worms	Acquiring distributed resources
Virus attacks	Attaching to programs and replicating
Bypasses	Avoiding authentication and authority
Trapdoor attacks	Utilizing existing flaws
Authorization attacks	Password cracking, hacking tokens
Active Misuse	Writing, using, with apparent authorization
Basic active misuse	Creating, modifying, using, denying service, entering false or misleading data
Incremental attacks	Using salami attacks
Denials of service	Perpetrating: saturation attacks
Passive Misuse	Reading with apparent authorization
Browsing	Making random or selective searches
Interference, aggregation	Exploiting database inferences and traffic analysis
Covert channels	Exploiting covert channels or other data leakage
Inactive Misuse	Willfully failing to perform expected duties or committing errors of omission
Indirect Misuse	Preparing for subsequent misuses, as in off-line pre-encryptive matching, factoring large numbers to obtain private keys, autodialer scanning

Reprinted with permission from "Computer-Related Risks," by P. Neumann, 1995, p. 30. Copyright 1995 by New York, NY: Addison-Wesley Publishing Company.

Appendix C: Characteristics of Decision Strategies

Characteristics of Decision Strategies

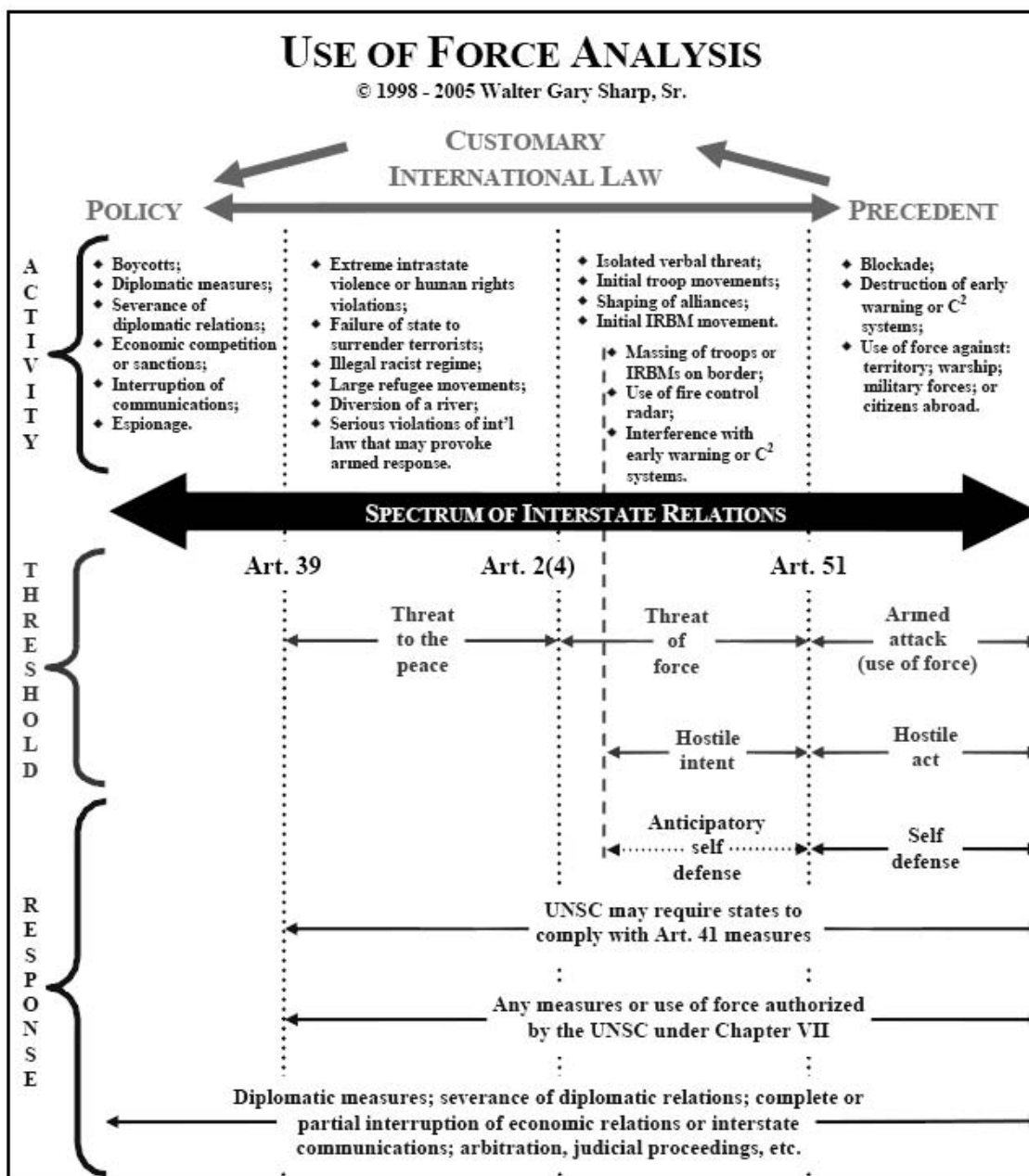
Decision	Model Type	Decision Strategy	Extensive/ Limited	Consistent/ Selective	Alternative/ Attribute	Compensatory/ Noncompensatory
Normative	Choice Models under Risk	Expected utility	Extensive	Consistent	Alternative	Compensatory
		Subjective expected utility	Extensive	Consistent	Alternative	Compensatory
		Prospect theory	Extensive	Consistent	Alternative	Compensatory
		Regret theory	Extensive	Consistent	Alternative	Compensatory
Behavioral	Riskless Choice Models	Weighted adding strategy	Extensive	Consistent	Alternative	Compensatory
		Equal weight strategy	Extensive	Consistent	Alternative	Compensatory
		Majority of confirming dimensions strategy	Extensive	Consistent	Attribute	Compensatory
		Lexicographic strategy	Limited	Selective	Attribute	Noncompensatory
		Satisficing strategy	Variable	Selective	Alternative	Noncompensatory
		Elimination by aspects Strategy	Variable	Selective	Attribute	Noncompensatory
		Conjunctive strategy	Extensive	Selective	Alternative	Noncompensatory
		Disjunctive strategy	Extensive	Selective	Alternative	Noncompensatory
Naturalistic	Process Models	Situation assessment Model	Decision Timeframe Changes in Different Contexts	Selective	These models do not utilize this theoretical construct	
		Recognition-primed decisions		Selective		
		Explanation-based decisions		Selective		
		Dominance search model		Selective	Both	Both
		Image theory		Selective	Both	Both

Adapted with permission from “Decision Theory: Poised for the New Millennium,” by W. Shao, A. Lye, S. Rundle-Thiele, and C. Fausnaugh, 2003, ANZMAC 2003 Adelaide Conference Proceedings, p. 685.

Copyright 2003 by Australian & New Zealand Marketing Academy.

Appendix D: Use of Force Analysis Spectrum

Use of Force Analysis Spectrum



Reprinted with permission from "Cyberspace and the Use of Force," by G. Sharp, 1999a, p. 78-79.

Modified by the author in 2005. Copyright 1999 by Falls Church, VA: Aegis Research Corporation.

Appendix E: Letter of Solicitation and Full Disclosure

Letter of Solicitation and Full Disclosure

I am a student at the University of Phoenix, completing a Doctorate of Management in Organizational Leadership with a specialization in Information Systems and Technology. I am conducting a research study entitled *Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers*. The purpose of this qualitative, phenomenological research study will be to explore the decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack. I have permission to conduct this research study from the Historian of the Joint Staff.

To accomplish the research study's goals, I seek your assistance. If you would like to participate in the study, please verify you meet the following criteria and contact me in order for us to establish an interview appointment.

- Senior military officer (pay grades O5 and above)
- Serve on the staff of the Joint Chiefs of Staff
- Assigned to one of the following directorates: J2, J3, J5, J6, J7, or J8
- Assigned to a division with a cyber warfare portfolio

Your participation will involve answering open-ended questions associated with your perceptions and experiences regarding the decision-making uncertainty factors associated with cyber warfare and the use of force. Your permission to digitally, audio record the interview will be required. I will transcribe our recorded interview in order to provide the data needed for analysis. Your participation in this study is voluntary. If you choose not to participate or to withdraw from the study at any time, you can do so without penalty or loss of benefit to yourself. The results of the research study may be published but your identity will remain confidential and your name will not be disclosed to any outside party.

The interview will take approximately 1 hour and will be conducted face-to-face if possible; however, telephone interviews are also allowed. The questions, answers, and recorded data must remain unclassified, releasable, and publishable. Your answers will be based on your individual perceptions and experiences and do not reflect the official position of your individual Military Department, the Joint Staff, the Department of Defense, or the U.S. government. The interview data will be reviewed by the Joint Staff, Director of Office Management to ensure compliance with Department of Defense rules and regulations regarding potentially sensitive material and to ensure the data are unclassified.

In this research, there are no foreseeable risks. Although there may be no direct benefit to you, a possible benefit of your participation is a better understanding of the uncertainties associated with the decision-making processes used by military leaders following a cyber attack. If you have any questions concerning the research study, please call me at (XXX) XXX-XXXX (or (XXX) XXX-XXX) and e-mail me at XXXX@email.phoenix.edu (or XXXX@navy.mil). If you wish to participate, the enclosed demographic questionnaire and informed consent form must be completed and returned to me prior to the interview.

Sincerely,

Daryl L. Caudle, CAPT, USN
Doctoral Student
University of Phoenix

Appendix F: Informed Consent Form

University of Phoenix

Informed Consent: Participants 18 years of age and older

Dear _____,

My name is Daryl L. Caudle, CAPT, USN and I am a doctoral student at the University of Phoenix. I am conducting a research study entitled Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers. The purpose of this qualitative, phenomenological research study will be to explore the decision-making uncertainty that senior military officers experience when determining the appropriate response to a cyber attack. I have permission to conduct this interview from the Historian of the Joint Staff.

Your participation will involve answering open-ended questions associated with your perceptions and experiences regarding the decision-making uncertainty factors associated with cyber warfare and the use of force. Your participation in this study is voluntary. If you choose not to participate or to withdraw from the study at any time, you can do so without penalty or loss of benefit to yourself. The results of the research study may be published but your identity will remain confidential and your name will not be disclosed to any outside party.

In this research, there are no foreseeable risks. Although there may be no direct benefit to you, a possible benefit of your participation is a better understanding of the uncertainties associated with the decision-making process used by military leaders following a cyber attack. If you have any questions concerning the research study, please call me at (XXX) XXX-XXXX (or (XXX) XXX-XXXX) or e-mail me at XXXX@email.phoenix.edu (or XXXX@navy.mil).

As a participant in this study, you should understand the following:

1. You may decline to participate or withdraw from participation at any time without consequences.
2. Your identity will be kept anonymous.
3. Daryl L. Caudle, the researcher, has thoroughly explained the parameters of the research study and all of my questions and concerns have been addressed.
4. You must grant permission for the researcher, Daryl L. Caudle, to digitally, audio record the interview. You understand that the information from the recorded interviews will be transcribed by the researcher. The researcher will structure a coding process to assure the anonymity of your name and protect the confidentiality of your responses.
5. Data will be stored in a secure and locked area. The data will be held for a period of three years, and then destroyed.
6. Questions, answers, and recorded data will be unclassified, releasable, and publishable.
7. Answers will be based on your individual perceptions and experiences and do not reflect the official position of your individual Military Department, the Joint Staff, the Department of Defense, or the U.S. government.

"By signing this form you acknowledge that you understand the nature of the study, the potential risks to you as a participant, and the means by which your identity will be kept confidential. Your signature on this form also indicates that you are 18 years old or older and that you give your permission to voluntarily serve as a participant in the study described."

Signature of the interviewee _____

Date _____

Signature of the researcher _____

Date _____

Appendix G: Joint Staff Interview Permission Form

UNIVERSITY OF PHOENIX

PERMISSION TO USE PREMISES, NAME, AND SUBJECTS

(Facility, Organization, University, Institution, or Association)

Joint Staff, Pentagon, Washington, DC

Check any that apply:

☒ I hereby authorize Daryl L. Caudle, CAPT USN, student of University of Phoenix, to use the premises (facility identified above) to conduct a study entitled Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers.

☒ I hereby authorize Daryl L. Caudle, CAPT, USN, student of University of Phoenix, to recruit subjects (Joint Staff military officers) for participation in a study entitled Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers.

☒ I hereby authorize Daryl L. Caudle, CAPT, USN, student of University of Phoenix, to use the name of the organization identified above when publishing results from the study entitled Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers.


Signature

13 Jan 2005
Date

David A. Armstrong, Ph.D.
BG USA (Ret.)
Historian of the Joint Staff
Joint Staff, Pentagon, Washington, DC 20301

Appendix H: Interview Data Collection Form

Interview Data Collection Form (1 of 2)

Demographic Questions

1. What is your gender?
2. What is your current age?
3. What is your current rank?
4. What is your education level?
5. What is your branch of Service?
6. How many years have you served in the military?
7. How many months have you served in a cyber warfare related position?
8. How would you describe your current cyber warfare related position?

9. What formal training have you had in cyber warfare?

10. What formal training have you had in traditional warfare?

Interview Data Collection Form (2 of 2)

Central Research Question

How do senior military officers perceive and describe the lived experience of decision-making uncertainty when determining the appropriate response to a cyber attack?

Lead Interview Question:

Please describe the decision-making uncertainty you experience when determining the appropriate response to a cyber attack.

Broad Guiding Questions:

1. Describe the dimensions, factors, and events associated with the experience.
2. Describe the people and organizations associated with the experience.
3. Describe your thinking process during the experience.
4. Describe your feelings and beliefs associated with the experience.
5. Describe any differences between individual experiences that stand out to you.
6. Have you shared all that is significant with regard to the experience?

Appendix I: Permission to Reuse Copyrighted Sources

Written Permission for Print and Electronic Reuse of Figure 3

29/07/2009 15:59

Page 1 of 2

**MONASH** University

Facsimile

Attention: [REDACTED]**Company:****Fax no:** [REDACTED]

Sender: Clayton School of Information Technology**Faculty:** Monash University**Fax no:** [REDACTED]

Pages: 2**Date:** Wednesday, 29 July 2009 at 3:58 PM**Subject:** [Image File] ,KMBT250, #274**FROM:**Image data has been attached to
the E-Mail.

Permission to Reproduce Copyrighted Source

I hereby permit Daryl Caudle to reproduce my image of Boyd's OODA loop model from my paper, "The Orientation Step of the OODA loop and Information Warfare" 2006.

Lachlan Brumley, Postgraduate Student, Monash University



July 29, 2009

Written Permission for Print and Electronic Reuse of Figure 4

07/29/2009 16:29

J ADDAMS & PARTNERS

PAGE 01/02



J. Addams & Partners, Inc.
500 Bishop Street
Studio B-5
Atlanta GA 30318

Date

29 July 2009

To

DARYL CAUDLE, CAPT USN

Organization

COMMANDER, SUB SQDN 3

From

CNET RICHARDS

Fax

Phone

Pages

2

Subject PERMISSION TO REPRINT

Message

Daryl - Good luck w/ your dissertation!

VR

PERSONAL AND CONFIDENTIAL

IMPORTANT NOTE: This message is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, and exempt from disclosure under applicable law.

If you are not the recipient name above, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is hereby prohibited. If you receive this communication in error, please notify us immediately by telephone and return the original message to us at the address above via the US Postal Service. Thank you.

07/29/2009 16:29

J ADDAMS & PARTNERS

PAGE 02/02

From: "Daryl L. Caudle" [REDACTED]
 Subject: Re: Permission Request to Reproduce Copyrighted Source
 Date: July 27, 2009 11:50:59 AM EDT
 To: Chet Richards [REDACTED]

Dear Mr. Richards,

After further discussing the requirements the University of Phoenix requires for the reprinting/reproducing previously published material for print and electronic reuse, I require a signed copy of your permission. I respectfully request you print and sign this e-mail to meet this requirement along with your typed name, title, and date. The fax number(s) are [REDACTED]. The receiving organization is Commander, Submarine Squadron Three, Pearl Harbor, HI. I apologize for this inconvenience. Thank you so much for your time and efforts in supporting my doctoral research.

Sincerely,

Daryl Caudle

Daryl L. Caudle, PE
 CAPT USN
 University of Phoenix Online
 [REDACTED]

----- Original Message -----

From: Chet Richards
 To: Daryl L. Caudle
 Sent: Friday, July 10, 2009 6:15 PM
 Subject: Re: Permission Request to Reproduce Copyrighted Source

Dear CAPT Caudle,

This will serve as permission to reprint or reproduce "The Modified OODA Loop" figure.

Best regards,
 Chet Richards

On Jul 10, 2009, at 4:40 PM, Daryl L. Caudle wrote:

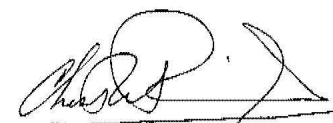
Dear Defense and the National Interest,

My name is Daryl L. Caudle, CAPT, USN and I am a doctoral student at the University of Phoenix. I am conducting a research study entitled Decision-Making, Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers. The purpose of the qualitative, phenomenological research study is to explore the central phenomenon of uncertainty in the decision-making process that senior military officers experience when considering if the response to a cyber attack warrants the use of force.

I would like to use the *The Modified OODA Loop* figure in J. R. Boyd's "An essay on winning and losing." In accordance with APA requirements and University of Phoenix policy, I require written permission to reprint/reproduce for print and electronic reuse. This e-mail serves as my official request to reprint/reproduce *The Modified OODA Loop* in my dissertation. Your permission (via e-mail) as the copyright holder would be much appreciated.

Sincerely,

Daryl Caudle
 Daryl L. Caudle, PE
 CAPT USN
 Assistant Deputy Director
 Information and Cyberspace Policy
 Joint Staff (J5)
 University of Phoenix Online
 [REDACTED]


 CHET W. RICHARDS
 Owner, Defense and the National Int.
 29 July 2009

Written Permission for Print and Electronic Reuse of Figure 5

From:

07/29/2009 16:08

#399 P.001/003

To: CAPT Caudle**Wingfield, Thomas CIV USA**

To: Daryl L. Caudle

Classification: UNCLASSIFIED

Caveats: NONE

Daryl,

No problem at all. A signed copy of this e-mail, including name, title, and date, will be faxed to COMSUBRON THREE today.

Please let me know what other support I can provide as you continue your work.

--Tom

-----Original Message-----

From: Daryl L. Caudle [REDACTED]

Sent: Monday, July 27, 2009 12:04 PM

To: Wingfield, Thomas CIV USA

Subject: Re: Permission Request to Reproduce Copyrighted Source

Dear Dr. Wingfield,

After further discussing the requirements the University of Phoenix requires for the reprinting/reproducing previously published material for print and electronic reuse, I require a signed copy of your permission. I respectfully request you print and sign this e-mail to meet this requirement along with your typed name, title, and date. The fax number(s) are [REDACTED]. The receiving organization is Commander, Submarine Squadron Three, Pearl Harbor, HI. I apologize for this inconvenience. Thank you so much for your time and efforts in supporting my doctoral research.

Sincerely,

Daryl Caudle

Daryl L. Caudle, PE

CAPT USN

University of Phoenix Online
[REDACTED]

[REDACTED] (Cell Work)

----- Original Message -----

From: "Wingfield, Thomas CIV USA" [REDACTED]
[REDACTED]

From:

07/29/2009 16:08

#399 P.002/003

To: "Michael, James (Bret) (CIV)" [REDACTED]
 "Duminda Wijesekera" [REDACTED]

"Daryl L. Caudle"

Sent: Friday, July 10, 2009 10:46 AM

Subject: RE: Permission Request to Reproduce Copyrighted Source (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Daryl,

Of course--you have my permission. Please let me know if there is anything else I can do to help!

--Tom

> ----- Original Message -----

> From: Daryl L. Caudle

> To: [REDACTED]

> Sent: Tuesday, July 07, 2009 1:00 AM

> Subject: Permission Request to Reproduce Copyrighted Source

>

>

> Dear Dr. Wingfield,

>

> My name is Daryl L. Caudle, CAPT, USN and I am a doctoral
 > student at the University of Phoenix. I am conducting a research
 > study entitled Decision-Making Uncertainty and the Use of Force in
 > Cyberspace: A Phenomenological Study of Military Officers. The
 > purpose of the qualitative, phenomenological research study is to
 > explore the central phenomenon of uncertainty in the decision-
 > making process that senior military officers experience when
 > considering if the response to a cyber attack warrants the use of
 > force.

>

>

> I would like to use the Figure 2: Decision Tree in Chapter 23,
 > "Making Decisions about Legal Responses to Cyber Attacks," in
 > Advances in Digital Forensics, 2006, p. 290 by L. Peng, T.
 > Wingfield, D. Wijesekera, E. Frye, R. Jackson and J. Michael. In
 > accordance with APA requirements and University of Phoenix policy,
 > I require written permission to reprint/reproduce for print and
 > electronic reuse. This e-mail serves as my official request to
 > reprint/reproduce Figure 2: Decision Tree in my dissertation.
 > Your permission as the copyright holder would be much appreciated.

>

>

>

> Sincerely,

>

>

>

> Daryl Caudle

>

>

>

From:

07/29/2009 16:09

#399 P.003/003

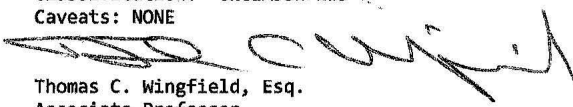
> Daryl L. Caudle, PE
> CAPT USN
>
> Assistant Deputy Director
>
> Information and Cyberspace Policy
>
> Joint Staff (J5)
> University of Phoenix Online
>

[REDACTED]
[REDACTED] (Cell Work)

>
>
>
>
>
>

Classification: UNCLASSIFIED
Caveats: NONE

Classification: UNCLASSIFIED
Caveats: NONE

 29 Jul 09
Thomas C. Wingfield, Esq.
Associate Professor
Department of Joint, Interagency, and Multinational Operations
US Army Command and General Staff College
9625 Belvoir Road, Room 185
Fort Belvoir, Virginia 22060 USA
[REDACTED]

Written Permission for Print and Electronic Reuse of Appendix B

07/28/2009 14:08

SRI INTL

PAGE 01

COMMANDER, SUBM. SQUADRON THREE, PEARL HARBOR
 To: "Daryl L. Caudle" [REDACTED] FAX [REDACTED]
 From: "Peter G. Neumann" [REDACTED]
 Subject: Re: Permission Request to Reproduce Copyrighted Source
 Date: Mon, 27 Jul 2009 11:59:58 -0400

Daryl, This message authorizes you to reuse in your dissertation the Table 3.1, Types of Computer Misuse, from my book, Computer-Related Risks. You have confirmed by e-mail that this is indeed the table that you wish to use, even though the caption is different from what appears below in your request. I hope you will give me access to your thesis when it is finished. Best wishes, Peter G. Neumann

Peter G. Neumann
 Principal Scientist
 Computer Science Lab
 SRI International EL-243
 333 Ravenswood Ave
 [REDACTED]
 [REDACTED]

Peter G. Neumann
 28 Jul 2009

YOU WROTE:
 Dear Dr. Neumann,

After further discussing the requirements the University of Phoenix requires for the reprinting/reproducing previously published material for print and electronic reuse, I require a signed copy of your permission. I respectfully request you print and sign this e-mail to meet this requirement along with your typed name, title, and date. The fax number(s) are [REDACTED]. The receiving organization is Commander, Submarine Squadron Three, Pearl Harbor, HI. I apologize for this inconvenience. Thank you so much for your time and efforts in supporting my doctoral research. *[Handwritten arrow pointing to "The receiving organization"]*

Sincerely,

Daryl Caudle

Daryl L. Caudle, PE
 CAPT USN
 University of Phoenix Online
 [REDACTED]
 [REDACTED] (Cell Work)

----- Original Message -----=20
 From: "Peter G. Neumann" [REDACTED]
 To: "Daryl L. Caudle" [REDACTED]
 Cc: [REDACTED]
 Sent: Thursday, July 09, 2009 7:39 AM
 Subject: Re: Permission Request to Reproduce Copyrighted Source

> You certainly have my permission.
 > I cannot give you WRITTEN permission until I return to SRI
 > in 11 days, but if you PRINT out this e-mail message, it might suffice
 > because it would be PRINTED.

----- Original Message -----=20

07/28/2009 14:08 [REDACTED]

SRI INTL

PAGE 02

From: Daryl L. Caudle=20
To: [REDACTED]
Sent: Wednesday, July 08, 2009 9:44 PM
Subject: Permission Request to Reproduce Copyrighted Source

Dear Dr. Neumann,=20

My name is Daryl L. Caudle, CAPT, USN and I am a doctoral student at the University of Phoenix. I am conducting a research study entitled Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers. The purpose of the qualitative, phenomenological research study is to explore the central phenomenon of uncertainty in the decision-making process that senior military officers experience when considering if the response to a cyber attack warrants the use of force.

I would like to use your table entitled Computer Network Attack Tools and Techniques in "Computer-Related Risks," 1995, by P. Neumann. In accordance with APA requirements and University of Phoenix policy, I require written permission to reprint/reproduce for print and electronic reuse. This e-mail serves as my official request to reprint/reproduce the Computer Network Attack Tools and Techniques table in my dissertation. Your permission as the copyright holder would be much appreciated.

Sincerely,

Daryl L. Caudle, PE
CAPT USN
Assistant Deputy Director
Information and Cyberspace Policy
Joint Staff (J5)

[REDACTED]
[REDACTED] (Cell Work)

Written Permission for Print and Electronic Reuse of Appendix C

Page 2 of 3

Daryl L. Caudle, PE
CAPT USN
University of Phoenix Online

----- Original Message -----

From: Daryl L. Caudle
To: Carolyn Fausnaugh
Sent: Monday, July 27, 2009 11:48 AM
Subject: Re: Permission Request to Reproduce Copyrighted Source

Dear Dr. Fausnaugh,

After further discussing the requirements the University of Phoenix requires for the reprinting/reproducing previously published material for print and electronic reuse, I require a signed copy of your permission. I respectfully request you print and sign this e-mail to meet this requirement along with your typed name, title, and date. The fax number(s) are [REDACTED]. The receiving organization is Commander, Submarine Squadron Three, Pearl Harbor, HI. I apologize for this inconvenience. Thank you so much for your time and efforts in supporting my doctoral research.

Sincerely,

Daryl Caudle

Daryl L. Caudle, PE
CAPT USN
University of Phoenix Online

----- Original Message -----

From: "Carolyn Fausnaugh"
To: "Daryl L. Caudle"
Sent: Saturday, July 11, 2009 8:31 AM
Subject: RE: Permission Request to Reproduce Copyrighted Source

Requested permission is granted. May we have an electronic copy of your dissertation upon its completion?

C. Fausnaugh

From: Daryl L. Caudle
Sent: Friday, July 10, 2009 4:32 PM
To: Carolyn Fausnaugh
Subject: Permission Request to Reproduce Copyrighted Source

8/5/2009
Aug. 05 2009 05:39PM PT

FROM : FLORIDA TECH SCH OF BUSINESS : PHONE NO. : [REDACTED]

*Permission Granted
Carolyn Fausnaugh
Assistant Professor
College of Business
Florida Institute
of Technology
8/5/2009*

Dear Dr. Fausnaugh,

My name is Daryl L. Caudle, CAPT, USN and I am a doctoral student at the University of Phoenix. I am conducting a research study entitled Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers. The purpose of the qualitative, phenomenological research study is to explore the central phenomenon of uncertainty in the decision-making process that senior military officers experience when considering if the response to a cyber attack warrants the use of force.

I would like to use the Appendix 1: Characteristics of Decision Strategies in the paper, "Decision Theory: Poised for the New Millennium," 2003, by W. Shao, A. Lye and S. Rundle-Thiele, and C. Fausnaugh. In accordance with APA requirements and University of Phoenix policy, I require written permission to reprint/reproduce for print and electronic reuse. This e-mail serves as my official request to reprint/reproduce Appendix 1: Characteristics of Decision Strategies in my dissertation. Your permission (via e-mail) as the copyright holder would be much appreciated.

Sincerely,

Daryl Caudle

Daryl L. Caudle, PE
CAPT USN
Assistant Deputy Director
Information and Cyberspace Policy
Joint Staff (J5)
University of Phoenix Online

Aug. 05 2009 25:40PM PT
8/5/2009

FROM : FLORIDA TECH SCH OF BUSINESS : PHONE NO. : [REDACTED]

Carolyn J. Fausnaugh, PhD, CPA
Assistant Professor
College of Business
Florida Institute of Technology
150 W. University Blvd
Melbourne, Florida 32901



FROM : FLORIDA TECH SCH OF BUSINESS
PHONE NO. : [REDACTED]
Aug. 05 2009 25:39PM PT

Written Permission for Print and Electronic Reuse of Appendix D

AUG-05-2009 17:20

OGC INTEL

P.001

Sharp, Gary, Mr, DoD OGC**Subject:** RE: Permission Request to Reproduce Copyrighted Source

From: Sharp, Gary, Mr, DoD OGC
Sent: Wednesday, August 05, 2009 4:02 PM
To: 'Daryl L. Caudle'
Cc: Sharp, Gary, Mr, DoD OGC
Subject: RE: Permission Request to Reproduce Copyrighted Source
 Daryl,

I will fax this shortly to [REDACTED]

Best of luck --
 Gary

From: Daryl L. Caudle [REDACTED]
Sent: Monday, July 27, 2009 11:55 AM
To: Walter Gary Sharp, Sr.
Cc: Sharp, Gary, Mr, DoD OGC; [REDACTED]
Subject: Re: Permission Request to Reproduce Copyrighted Source

Dear Gary,

After further discussing the requirements the University of Phoenix requires for the reprinting/reproducing previously published material for print and electronic reuse, I require a signed copy of your permission. I respectfully request you print and sign this e-mail to meet this requirement along with your typed name, title, and date. The fax number(s) are [REDACTED]. The receiving organization is Commander, Submarine Squadron Three, Pearl Harbor, HI. I apologize for this inconvenience. Thank you so much for your time and efforts in supporting my doctoral research.

Sincerely,

Daryl Caudle

You have my my written permission to reprint/reproduce for print and electronic reuse my Use of Force Analysis figure in your dissertation.

Walter Gary Sharp, Sr.

Daryl L. Caudle, PE
 CAPT USN
 University of Phoenix Online

WALTER GARY SHARP, SR.
 SENIOR ASSOCIATE DEPUTY GENERAL COUNSEL, U.S. DoD
 AUGUST 5, 2009

----- Original Message -----

From: Walter Gary Sharp, Sr.
To: [REDACTED]
Cc: [REDACTED]
Sent: Friday, July 10, 2009 6:35 AM
Subject: Re: Permission Request to Reproduce Copyrighted Source

Daryl,

8/5/2009

AUG-05-2009 17:20

OGC INTEL

P.002

Yes, of course. Please consider this email as my written permission to reprint/reproduce for print and electronic reuse my Use of Force Analysis figure in your dissertation.

Best of luck -- and when you finish, I would love to read your dissertation.

v/r,
Gary

Walter Gary Sharp, Sr.
Senior Associate Deputy General Counsel, Intelligence
Office of the General Counsel, U.S. Department of Defense
1600 Defense Pentagon (Room 3B710)
Washington, DC 20301-1600

Email
Direct line
Reception
Fax
BlackBerry

CAUTION: Information contained in this message may be protected by the attorney/client, attorney work product, deliberative process or other privileges. Do not disseminate further without approval from the Office of the DoD General Counsel.

-----Original Message-----

From: Daryl L. Caudle
To:
Sent: Wed, Jul 8, 2009 8:54 pm
Subject: Permission Request to Reproduce Copyrighted Source

Dear Gary,

As you know, I am a doctoral student at the University of Phoenix conducting a research study entitled Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers.

I would like to use your Use of Force Analysis figure (attached) in my dissertation. In accordance with APA requirements and University of Phoenix policy, I require written permission to reprint/reproduce for print and electronic reuse. This e-mail serves as my official request to reprint/reproduce Use of Force Analysis figure in my dissertation. Your permission as the copyright holder would be much appreciated.

Hope all is going well with the cyber crew! Thanks again Gary.

Sincerely,

Daryl Caudle

Daryl L. Caudle, PE
CAPT USN
Assistant Deputy Director
Information and Cyberspace Policy
Joint Staff (J5)

8/5/2009

Appendix J: Rank Order of Invariant Constituents

Rank Order of Invariant Constituents

Rank Order	Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
1	Extent of Understanding Cyber Warfare	21	153
2	Lack of Response Options	20	152
3	Poor Understanding of Current Capabilities	20	148
4	Inadequate National Strategic Policy	20	118
5	Inadequate Legal Framework	20	115
6	Relative Level of Attribution Required	20	95
7	Complex Effects-based Operations	20	87
8	Unintended Higher Order Effects	20	68
9	Generational Differences	20	59
10	Instrument of National Power Legitimacy	20	42
11	Lack of Collaboration and Consensus	19	73
12	Military vs. Societal Cultures	19	58
13	Self-defense and Counter Attack	19	57
14	Ethical Warfare Considerations	19	56
15	Lack of Deterrent Consequences	19	53
16	Response Thresholds and Necessity	19	47
17	Untested Rules of Engagement	19	46
18	Attack Recognition and Categorization	18	61
19	Attack Severity Determination	18	59
20	Ubiquitous Domain of Warfare	18	56
21	Response Speed and Responsiveness	18	54

Rank Order	Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
22	Proportionality and Equivalence Determination	18	51
23	Response Process and Authority	17	70
24	Ineffective Command and Control	17	62
25	Multiple Actors and Motives	17	60
26	Insufficient Experience and Expertise	16	47
27	Lack of Formal Training Opportunities	16	43
28	Deconfliction and Synchronization	16	36
29	Complex and Chaotic Environment	15	56
30	Ill-defined Roles and Responsibilities	15	56
31	Lack of Education Institutional Curricula	15	36
32	Traditional Military Activity Extent	14	56
33	Inconsistent Information Valuation and Sharing	14	43
34	Immature Modeling and Simulations	14	34
35	Attack Motive and Context	14	31
36	Lack of Common Lexicon, Vernacular, and Meaning	14	29
37	Sovereignty and Jurisdiction Challenges	13	44
38	Critical Infrastructure Dependency	13	43
39	Privacy, Anonymity, and Civil Liberty Concerns	13	35
40	Operational Gain vs. Intelligence Loss	12	46
41	Rules of War Applicability	12	25
42	Undeveloped Cyber Warfare Doctrine	12	24

Rank Order	Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
43	Centralized vs. Decentralized Constructs	12	22
44	Open and Boundaryless Commons	11	26
45	Target Discrimination and Distinction	11	20
46	Planning and Targeting Processes	11	19
47	Interdependent Communication Medium	10	25
48	Damage Assessment Methods	10	17
49	Varied Perceptions, Values, and Beliefs	9	30
50	Insurgent Area of Hostility and Crime	9	21
51	Insufficient National Resources and Debate	9	19
52	Overly Classified and Compartmentalized	9	18
53	Hostile Intent and Act of War Definitions	9	17
54	Lack of Political Resolve and Transparency	9	15
55	Dehumanizing Cyber Warfare	8	23
56	Virtual and Physical Duality	8	18
57	Fog of War and Deception	8	17
58	Antiquated International Treaties	8	17
59	Criminal Activity vs. Information Warfare	8	14
60	Current Conflict Posture Considerations	8	13
61	Integrating and Normalizing Operations	7	31
62	Social and International Behavioral Norms	7	20

Rank Order	Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
63	Risk of Escalation and Cyber Arms Race	7	20
64	Ambiguous Vulnerabilities	7	19
65	Proxies and Identification Authentication	7	14
66	Kinetic Attack Analogy and Equivalence	7	13
67	Lack of Access and Situational Awareness	7	13
68	Forensic and Data Credibility Challenges	7	12
69	Government Stakeholders and Conflicting Equities	7	11
70	Evolving Level of Readiness	6	14
71	Attack Capacity and Precision	6	13
72	Laws of Armed Conflict Applicability	6	9
73	Data Ownership and Intellectual Property	5	24
74	Catastrophic Cyber Event Required	5	11
75	Inadequate Self-Confidence	5	6
76	Response Scalability	5	5
77	Inadequate Technology Exposure and Utilization	4	18
78	Academic vs. Commercial Cultures	4	7
79	Attack Covertiness and Validity	4	6
80	Unrealistic and Nonintegrated Exercises	4	6
81	Ineffective Governance, Compliance, and Controls	4	6
82	Autonomous Response Capability	4	4

Rank Order	Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
83	Levels of Resiliency and Security	3	13
84	Irregular Warfare and Low Cost of Entry	3	4
85	Insufficient Research and Development	2	8
86	Poor Anticipatory and Proficiency Skills	2	6
87	Ambiguous Leadership Vision and Accountability	2	5

Appendix K: Key Themes and Supporting Invariant Constituents

Key Themes and Supporting Invariant Constituents

Theme 1: Response Characteristics and Efficacy Considerations

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Lack of Response Options	20	152
Response Thresholds and Necessity	19	47
Response Speed and Responsiveness	18	54
Proportionality and Equivalence Determination	18	51
Response Process and Authority	17	70
Target Discrimination and Distinction	11	20
Response Scalability	5	5
Autonomous Response Capability	4	4
Weighted Average Text Segments: 65		

Theme 2: Social, Behavioral, Cultural, and Cognitive Aspects

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Extent of Understanding Cyber Warfare	21	153
Generational Differences	20	59
Military vs. Societal Cultures	19	58
Lack of Common Lexicon and Meaning	14	29
Varied Perceptions, Values, and Beliefs	9	30
Dehumanizing Cyber Warfare	8	23
Social and International Behavioral Norms	7	20
Inadequate Self-Confidence	5	6
Academic vs. Commercial Cultures	4	7
Weighted Average Text Segments: 61		

Theme 3: Policy and Strategic Aspects

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Inadequate National Strategic Policy	20	118
Relative Level of Attribution Required	20	95
Instrument of National Power Legitimacy	20	42
Lack of Deterrent Consequences	19	53
Untested Rules of Engagement	19	46
Multiple Actors and Motives	17	60
Operational Gain vs. Intelligence Loss	12	46
Insufficient National Resources and Debate	9	19
Lack of Political Resolve and Transparency	9	15
Current Conflict Posture Considerations	8	13
Risk of Escalation and Cyber Arms Race	7	20
Weighted Average Text Segments: 58		

Theme 4: Legal and Ethical Aspects

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Inadequate Legal Framework	20	115
Ethical Warfare Considerations	19	56
Sovereignty and Jurisdiction Challenges	13	44
Privacy, Anonymity, and Civil Liberty Concerns	13	35
Hostile Intent and Act of War Definitions	9	17
Antiquated International Treaties	8	17
Laws of Armed Conflict Applicability	6	9
Ineffective Governance, Compliance, and Controls	4	6
Weighted Average Text Segments: 52		

Theme 5: Organizational Concepts, Constructs, and Relational Considerations

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Lack of Collaboration and Consensus	19	73
Ineffective Command and Control	17	62
Ill-defined Roles and Responsibilities	15	56
Centralized vs. Decentralized Constructs	12	22
Government Stakeholders and Conflicting Equities	7	11
Ambiguous Leadership Vision and Accountability	2	5
Weighted Average Text Segments: 50		

Theme 6: Data, Information, and Technology Considerations

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Poor Understanding of Current Capabilities	20	148
Inconsistent Information Valuation and Sharing	14	43
Immature Modeling and Simulations	14	34
Overly Classified and Compartmentalized	9	18
Criminal Activity vs. Information Warfare	8	14
Proxies and Identification Authentication	7	14
Lack of Access and Situational Awareness	7	13
Forensic and Data Credibility Challenges	7	12
Data Ownership and Intellectual Property	5	24
Inadequate Technology Exposure and Utilization	4	18
Insufficient Research and Development	2	8
Weighted Average Text Segments: 49		

Theme 7: Cyber Attack Characteristics

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Unintended Higher Order Effects	20	68
Attack Recognition and Categorization	18	61
Attack Severity Determination	18	59
Attack Motive and Context	14	31
Kinetic Attack Analogy and Equivalence	7	13
Attack Capacity and Precision	6	13
Attack Covertiness and Validity	4	6
Weighted Average Text Segments: 48		

Theme 8: Cyber Warfare Characteristics

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Complex Effects-based Operations	20	87
Self-defense and Counter Attack	19	57
Deconfliction and Synchronization	16	36
Traditional Military Activity Extent	14	56
Rules of War Applicability	12	25
Planning and Targeting Processes	11	19
Damage Assessment Methods	10	17
Fog of War and Deception	8	17
Integrating and Normalizing Operations	7	31
Evolving Level of Readiness	6	14
Catastrophic Cyber Event Required	5	11
Irregular Warfare and Low Cost of Entry	3	4
Weighted Average Text Segments: 41		

Theme 9: Cyberspace Characteristics

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Ubiquitous Domain of Warfare	18	56
Complex and Chaotic Environment	15	56
Critical Infrastructure Dependency	13	43
Open and Boundaryless Commons	11	26
Interdependent Communication Medium	10	25
Insurgent Area of Hostility and Crime	9	21
Virtual and Physical Duality	8	18
Ambiguous Vulnerabilities	7	19
Levels of Resiliency and Security	3	13
Weighted Average Text Segments: 37		

Theme 10: Experience, Training, and Education Considerations

Invariant Constituents	Interviews Containing Invariant Constituent	Text Segments Coded to Invariant Constituent
Insufficient Experience and Expertise	16	47
Lack of Formal Training Opportunities	16	43
Lack of Education Institutional Curricula	15	36
Undeveloped Cyber Warfare Doctrine	12	24
Unrealistic and Nonintegrated Exercises	4	6
Poor Anticipatory and Proficiency Skills	2	6
Weighted Average Text Segments: 35		

Appendix L: Individual Textual Descriptions

Individual Textual Descriptions

Individual textual descriptions capture the participants' unique perceptions, insights, and accountings of the decision-making uncertainty experienced when determining the appropriate response to a cyber attack. The participants' transcribed interviews, audio files, and field notes were reviewed to develop the individual textual descriptions. The textual descriptions support understanding "what" the senior military officers experienced when encountering the central phenomenon (Moustakas, 1994).

Textual Description Summary for Participant #1 (DS240004)

Participant #1 described the experience of decision-making uncertainty following a cyber attack to be primarily the result of a lack of understanding of the available response options and capabilities. "You know we don't know all the response tools available. I think to be able to understand the tools available as a military leader, I'm speaking specifically cyber tools, to determine if a response in kind is appropriate or some other response is necessary." Participant #1 added, "We don't understand that as a government, or military or a nation that if we get cyber attacked . . . how to respond with an appropriate response because I don't think we understand."

Participant #1 was also concerned with the legal framework governing cyber warfare. "The current laws don't handle the whole concept of cyberspace operations well because it's based upon . . . sovereign territory and . . . having the ability to place a value on information." Participant #1 expressed, "We don't know if an attack is from a nation state, an event from an actor that is working alone, or a criminal actor and so that requires understanding different legal constructs . . . such as Title 10, Title 50 and Title 18 when making decisions."

Participant #1 described the importance of attribution (i.e., precisely determining the source or actor) when making response decisions following a cyber attack. “Is a hundred percent [attribution] required, no but there’s got to be some sort of attribution before the use of force is authorized.” Participant #1 described that information sharing, collaboration, and jurisdiction are essential elements of attribution. “The information sharing problems we have with the intelligence community, the military, private industry, and law enforcement hinders our ability to attribute a cyber attack.” With respect to jurisdiction, Participant #1 noted, “If the attack is criminal, it’s more likely going to be the FBI who takes the lead on it, where if we considered it a nation state act, or a terrorist act, then clearly it would be more of a military like response.”

Textual Description Summary for Participant #2 (DS240005)

Participant #2 described the experience of decision-making uncertainty following a cyber attack to be centered on inadequate understanding of cyber warfare and inconsistent semantics associated with the lack of a common lexicon. “The word attack has an understood meaning, which implicitly merits a use of force response. But, for a cyber attack, one must assign meaning a part from the word or phrase itself . . . because military leaders require unambiguous meaning for the words they use.” Participant #2 added, “The decision-making process for responding with force to a cyber attack is impeded at the outset because the phrase cyber attack has no meaningful utility unless it’s understood to mean only that a person has wielded a weapon with the intent to kill.” Regarding the common lexicon perceptions, Participant #2 noted, “It’s a semantics argument or a definitional problem because I think the use of the phrase ‘cyber attack’

has such a large variance of meanings that it's almost useless in its existing construct . . . unless we can lessen the ambiguity.”

Participant #2 also described the significance attribution and equivalence have when categorizing cyber attacks as EBO. “One factor is who did it? Military leaders rightfully seek to eliminate uncertainty as to who did the act when they're considering the use of hostile force or use of force in response to a cyber attack. However, the need to attribute does not and should not impede a decision to use force in response to an attack once the instigator is identified.” On the concept of equivalence, Participant #2 observed, “If I have equivalent activities, you know, whether it be cyber or physical, context is key. Therefore, by equivalent . . . a kinetic and a cyber attack have the same effect.” Following a cyber attack, Participant #2 conveyed, “I going to take responses that mitigate the effects, recover from the effects, and describe the effects in detail including the source of the device and who did it.”

Textual Description Summary for Participant #3 (DS240006)

Participant #3 described the experience of decision-making uncertainty following a cyber attack predominately based on the lack of defined organizational roles and responsibilities and the reluctance to use cyber warfare as an instrument of national power. Participant #3 observed, “Different agencies have different interests, different perceptions of their responsibilities and roles and it's very difficult to act promptly and precisely when you have consensus based organizations in which any member, whether with good intentions or not, can confound the [decision] process that you would not have with a kinetic strike.” Further, Participant #3 believed, “Cyber power is an element of national power. We're certainly dependent on it [Internet] and so we need to make sure .

. . we have a defense for it and we have an offense for it as well, but again, in conjunction with the other elements of national power.”

Participant #3 also expressed that decision-making uncertainty is influenced by insufficient response speed, loosely defined thresholds, and a poor understanding of existing capabilities. “The speed of the domain makes appropriate assessment and rapid action absolutely critical, but I think . . . we’re driven to say speed entices rational leaders to assume there’s some acceptance of rashness or recklessness and that’s not the case.” Regarding capabilities, Participant #3 questioned, “What are our choices? What are our options? What can we do? In cyberspace, the capabilities . . . are so highly classified and compartmentalized we often struggle knowing what we can do.” Participant #3 summarized, “It’s difficult to make response decisions without a value of data, without certainty of thresholds, without clarity of roles and missions, and it’s difficult for a decision maker to make a prudent choice when they don’t really understand what’s possible, technically.”

Textual Description Summary for Participant #4 (DS240007)

Participant #4 described the experience of decision-making uncertainty following a cyber attack based on the virtual nature of cyberspace and the dehumanization of cyber warfare through reversible attacks against a digital adversary. “Cyberspace is about a virtual concept that rapidly – to us, seems like a real person, we even use those terms, and it’s not. At the end of the day, if we conduct cyber operations, it’s just affecting information about something, it’s still not real, but we treat it as such.” With respect to reversibility, Participant #4 added, “The other thing that I think that comes along with the use of force that we really need to seriously consider in cyberspace is the concept of if we

can literally press the reset button and undo what we've done, was it really use of force? If it's reversible, the response to a cyber attack is not a real use of force."

Participant #4 also described that anonymity complicates attribution, self-defense and response speed. "I'm sure that I could be convinced that there are some cases when – talking about anonymity – I think it's absolutely essential to attribute an attack. I think it's a prerogative of cyberspace or a fundamental element of it, and I think trying to take away anonymity is creating an insurgency There is the analogy in the right to self-defense, and if I'm walking down the street of Fallujah and somebody starts shooting at me, the attribution does not have to get to how old is he, what is he dressed in, what does he look like, is it a he or a she, before I take responsive action. Attribution is not a point; it's an immediate response. So, I happen to believe and think that in cyberspace, that kind of retribution should be aside from attribution, attribution is a distraction. Attribution, at that level, is proof that people don't get the difference between what's real and what's virtual."

Textual Description Summary for Participant #5 (DS240008)

Participant #5 described the experience of decision-making uncertainty following a cyber attack based on the lack of response options and inadequate understanding of existing capabilities. "There is definitely a difference in responding [following a kinetic attack versus a cyber attack] . . . maybe not ultimately the type of response, but having several response options leaves a lot less ambiguity in the decision process." In addition, Participant #5 asserted, "We don't know what capabilities are available to us, what the options are fully. And, to get those options made aware – to become aware of what those

options are, we would have to go to the intelligence community to understand the full range of response options.”

Participant #5 also conveyed that decision-making uncertainty is influenced by the potential of a cyber arms race resulting from an ineffective cyber deterrence policy. “I think that there’s a very likely chance of an arms race in cyberspace about who’s got the better, fastest capability whether it is an offensive capability or a defensive capability, and that is the deterrent. I think until that is discovered and matured, I think there’s going to be the continual pushing of the envelope and a continual pursuit of the next best weapon capability.” Participant #5 continued, “There is an ongoing brinksmanship going on in cyberspace where a lot of players, whether groups or national states are active, and they continue to push the envelope. There will continue to be one-upmanship, and I think that in cyberspace we’re going to see that until someone comes up with the WMD of cyberspace.”

Participant #5 also noted that organizational cultures within the DoD and the existing command and control structure add uncertainty to the response decision process. “I think senior military leaders who are in the position to make decisions on the application of force in response to a cyber attack are not familiar with activities in the domain. There’s a layer of complexity there. I think, culturally, they still see problems with the networks as an organizational problem or a communications problem, not an operational problem.” Participant #5 perceived, “The command and control is not clean, and therefore, knowing who has categorized the attack in the right way, and who can authorize the use of force is often unclear.”

Textual Description Summary for Participant #6 (DS240009)

Participant #6 described the experience of decision-making uncertainty following a cyber attack based on the need to understand more fully the characteristics of response options including existing capabilities, higher order effects, damage assessment, and the determination of proportionality. “In deciding if a cyber attack warrants a use of force, you have to really consider . . . the extent of damage caused by a cyber attack. Another thing I thought about was, when faced with responding with a use of force to a cyber attack, you must consider how you’re going to respond. So, one of the uncertainty factors is the proportionality of that response, the secondary effects of retaliation – if it’s done through cyberspace – and thoughts towards escalation.” Concerning understanding capabilities, Participant #6 noted, “Decision-making processes are challenging – I’d say, technologically, because there are not many people, myself included, who understand fully what options are available. On the cyber side of warfare, I do not feel confident because I do not understand a lot of the technology and the tools that are associated with that.”

Participant #6 also expressed that decision-making uncertainty is influenced by how societal and anonymity factors create insurgency opportunities in cyberspace. “There are social cultural influences that affect the military in that the Internet technology and communications infrastructure and the like have been set up among society as a cultural lubricant – a way for us to communicate; something that makes our lives easier. However, the United States in general – Americans – do not perceive cyberspace as a vital element to our nation’s existence and as a critical element of national power.” Participant #6 further articulated, “I think the societal culture . . . fits an insurgency

[model] in that if a person doesn't take action to stop the extremist – actively take action – then they're passively allowing what they do – accepting it – and almost creating a societal norm to that culture. So, by Americans having a culture where the Internet can be used for whatever and shouldn't be regulated at all, they're almost creating a situation where it is allowable for other nation states or criminal activity to be empowered by anonymity.

Textual Description Summary for Participant #7 (DS240010)

Participant #7 described the experience of decision-making uncertainty following a cyber attack from an effects-based operational perspective in which the available response options and existing capabilities must be better understood. “As I'm thinking through it, I'm thinking effects-based is essential to any response. I mean, what effect are you trying to achieve in cyber? That also will allow you to determine intent because what I'm thinking is that to conduct cyber warfare you go back to the simple principles of war and the kinds of things, you know, maneuver and force, and I believe the effects must be the same.” Participant #7 pondered, “Do I have the capacity and the capability. In other words, do I have the forces, the trained forces to be able to respond, and do I have the expertise to respond in this kind of manner in the cyber world, in a cyber attack.”

Participant #7 voiced concerns that decision-making uncertainty is influenced also by inadequate modeling and training efforts in addition to the complexities created by the *fog of war* within the cyber domain. “Counter-insurgency is probably a model to be considered for this domain because operations are similar. Is it the right model? I don't know. I'm not sure we know what the right model is, and that's what we're struggling

with. Participant #7 added, “Of course training affects the cultural divide as it would any other kind of warfare domain. I mean that’s why . . . the military needs various levels of training in place to help shape your thinking as you continue to develop professionally.” Regarding the cyber domain, “I compare cyber warfare to just normal warfare. So, in a cyber world . . . the reconnaissance, the intelligence, the right site picture and situational awareness matter in order to make an informed decision . . . because it helps to clear some of the fog of war.”

Textual Description Summary for Participant #8 (DS240011)

Participant #8 described the experience of decision-making uncertainty following a cyber attack primarily from a legal perspective with emphasis on the need for a comprehensive understanding of available response options and existing capabilities. “From the legal standpoint, responding in cyberspace comes down to distinction, proportionality, and fact, you know, identification of the threat and source of the threat. What makes it a more difficult process in cyberspace is that generally speaking, when you have a kinetic attack, identification of the source of the attack tends to be much easier.” Participant #8 further articulated, “There is some legal analysis, but the critical factor in drawing the line for a response is the operators who can describe what capabilities they have to respond to a particular threat, and what those capabilities do for you. What’s the level of destruction? Therefore, very few of those [cyber warfare decisional] issues are legal issues. There is legal analysis to help draw that line, but they are policy calls.”

Participant #8 also stressed that decision-making uncertainty is influenced by the inherent right of self-defense and an ineffective response process. “Following a cyber

attack, similar to a kinetic attack, you have, under the right of self-defense, the ability to respond to that attack. So long as the response is proportional, which is actually a fairly drawn parameter, you don't have to respond to the attack in an exact parallel manner."

Participant #8 added, "First and foremost with respect to the decision-making process, the process in deciding how to respond to a cyber attack, the decision-makers utilize the same criteria, or should use the same criteria as a kinetic attack. The existing legal framework is the same, and should be the same for cyber as it is for kinetic. The fact that you're operating in a different medium doesn't change the essential legal framework, or the analytic process. The law informs the process, but it is not the process."

Therefore, Participant #8 also considered decision-making uncertainty to be driven by a lack of understanding. "So the real way to raise the tide, if you will, in terms of getting Commanders to be able to make the decisions is just like the training that officers and folks, military members, have on weapons capabilities, etc. You're going to have to develop a cyber-warrior force that knows enough about systems, available weapons, and available defenses to speak knowledgeably and do the necessary analysis." Participant #8 concluded, "What you have right now is a lack of familiarity, I think, that makes the reaction quite tentative. I think that will change as people develop experience."

Textual Description Summary for Participant #9 (DS240012)

Participant #9 described the experience of decision-making uncertainty following a cyber attack to be based on an insufficient understanding of organizational roles and responsibilities and the lack of an overall cyber warfare strategy. "Within the DoD, we really don't have a central organization at this point running cyberspace. Unlike ground

warfare, the Army has that. Air warfare, the Air Force has that. Cyber is spread across the Services. It's spread across the government agencies. Everyone feels they have a play in that. Everyone feels that they're in charge of their piece. Integrating that has been a difficult proposition. Again, there is no real central organization." Participant #9 continued, "We need to stand up an organization that would be charged with really pulling it all together – pulling together the strategy, and tactics of how we fight, and defend within cyberspace. Until that happens, I think we're going to continue doing things piecemeal But again, no comprehensive strategy, and approach in defending the overall, not only DoD, but U.S. network infrastructure, extended out to the Internet."

Participant #9 also conveyed that decision-making uncertainty is influenced by the capability to recognize a cyber attack and its severity. "I think it's really perception, and it boils down to the level of damage to infrastructure, to life and limb. You know, coming up in the military we're all taught that if life and limb are impact significantly, that is critical, and we would respond in kind." Participant #9 noted the need to determine operational impact following a cyber attack. "You really want to identify how the network going down impacts not only the current operations, but future operations as well. I think it's important to distinguish between losing life and cyber infrastructure. I think the uncertainty factor plays a key role. You may have a hostile actor, or a nation-state that is trying to infiltrate your networks to exfiltrate information that may end up causing loss of life and limb, and I think making that determination of the criticality of that data is [sic] a key factor."

Textual Description Summary for Participant #10 (DS240013)

Participant #10 described the experience of decision-making uncertainty following a cyber attack to be based on the inability to determine response options due to inadequate attack analysis capability, unclear lines of authority, and ineffective command and control processes. “If the network is attacked, what happened? By taking a system out or a portion of the network out, what were the real implications of that? Does it drive a need for a response, be it kinetic or otherwise? I think this lends a significant amount of uncertainty into any leader’s decision. And, the further you get away from the valued information, the more distorted it becomes. And it makes it harder for you to make a decision on what force response is required.” With respect to making decisions, Participant #10 stated, “From my experiences . . . I think a combat leader who wants to respond quickly uses the OODA [observe-orient-decide-act] loop approach. However, the OODA loop process gets confused because you’re not able to observe and orient yourself easily in cyberspace, and then making your decision becomes complicated.”

Participant #10 further noted, “I think other uncertainty stems from the confusion of roles. We’re still struggling to put a boundary around the network. And, what I mean by that is not necessarily a defense boundary, but whose area of responsibility is what. And, the overlaps. So, if a network was attacked in this sector, who has the jurisdiction to assess what happened, make a call on where the attack came from, and then determine who needs to generate the response. Without those lines, you’re missing . . . unity of command and control.” Regarding attack recognition and attribution, Participant #10 observed, “One of the problems you have first is assessing the origination of the attack. First and foremost, identifying the enemy if you will. There’s still a great deal of swirl

on how to do that based on my experiences. It's not always clear. Where is the attack coming from? Is this a legal issue or is this a military issue, in interest of national security?"

Textual Description Summary for Participant #11 (DS240014)

Participant #11 described the experience of decision-making uncertainty following a cyber attack by expressing the need for response options with emphasis on response speed, attack analysis, and thresholds. "I think there's uncertainty with particular activities and effects in cyberspace that we can say are 'redline' sorts of activities. There are some activities where you can say, 'If this happens, then I am going to respond.' But, the vast majority of, at least in my mind, of the impact of cyber activity, cyber attacks if you will – I think they fall into a gray area where the response may very well not be a response in kind. It may very well not be a kinetic response. It may not be a military response. And, part of the difficulty, I think is the challenge of understanding the depth and breadth of the impact. As you well know, it may be a very long time before you understand exactly what happened."

Participant #11 continued to describe, "In most cases, I would tend to think that centralizing decision-making authority will increase the responsiveness and decrease the time required to respond. The problem though, is that when you centralize decision-making authority, that organization is often far removed from the actual impact of the attack. If you have central decision-making authority, unless you have been given a certain degree of decision-making authority locally – rules of engagement, if you will, you've got to wait for the information to go up the chain of command." In addition, Participant #10 shared, "Concerning cyber warfare against a purely military target, I

believe it's absolutely ethical. Probably only in the concept of total war are you going to expand that concept to other national [computer] systems, whether it be financial or infrastructure. I think you really do cross a line there when you're talking about a total commitment of a nation when bringing those types of targets into play. I think response thresholds exist. I just honestly don't know where they're defined."

Textual Description Summary for Participant #12 (DS240015)

Participant #12 described the experience of decision-making uncertainty following a cyber attack from the perspective of more fully understanding the characteristics and dynamics of cyber warfare and the associated effects. "I think in the military construct, I believe cyber warfare is an ethical means of warfare. However, that comes with the large caveat that the military's understanding of cyber warfare would be related to the understanding of the domain and that that domain is a component of combined arms warfare. Another factor to consider is to understand that we may not necessarily always have to respond in kind. For example, our abilities to understand the consequences, the collateral effects, the collateral damage that's done by an attack. Whether we're talking about convention attacks, a military attack, or something diplomatic, economic, as far as cutting off diplomatic relations or creating embargos or any of the other tools that are available to the country. So I think a response to a cyber incident does not necessarily have to be accomplished using cyber."

In addition to concerns over the host of malicious actors and the risks associated with their cyber capabilities, Participant #12 shared, "If we're going to go down the road of a cyber based response action, then we're going to obviously want to have an understanding of what some of the outside collateral effects are going to be. So, when we

think that we're going to accomplish a response, we understand the unintended consequences. And, I think that we're fairly immature at being able to do that at this point, which is why most of the conversation that we have with regard to cyber attacks, cyber response action, tends to be factored in at the strategic level. Because we know that at some point in the future, we'll evolve to where we can understand responses at the tactical level and that the effects will stay within the tactical level as opposed to how we plan right now. Because of the great unknowns, we think that there are certainly strategic levels of effects that will bleed over and cause unintended consequences."

Textual Description Summary for Participant #13 (DS240016)

Participant #13 described the experience of decision-making uncertainty following a cyber attack based on the legal challenges associated with the attribution of malicious actors and the establishment of legitimate boundaries in cyberspace. "When you're looking at response decisions from the existing legal framework, I mean you really have to look at it from the point of view of a commander that's on the battlefield. Of course, if he has a cyber attack within his area of responsibility, then he has the ability to defend and protect himself. But, when you look at it from a perspective beyond the battlefield – and really cyber extends itself way beyond that small entity – you're getting into global networks across borders, across countries and different operations. Given that nuance, you have to consider the attack might have originated from somewhere in the United States. Hence, the legal challenges emerge when going from a battlefield area into the United States when making response decisions. The legal authority concerns are much more complex."

Participant #13 also expressed that decision-making uncertainty is influenced by inadequate capabilities that hinder cyber attack analysis and the response process.

“When you look at the whole idea of how the Internet is built, there is some ability to find destinations, find relocations, but there’s ways that you can mask. There’s ways that you can mask your movements in cyberspace, and in some cases the technology to find somebody is not necessarily keeping up with those abilities to move around cyberspace anonymously.” Considering the technology limitations, Participant #13 stated, “You determine the best courses of action based on your intelligence, based on the enemy’s location, and you choose the best course of action to attack or defend. So, I think that it’s no different in cyberspace. You have to make sure that you have laid out all the options and you take care – again, using all of your principle staff – to help you determine your decisions. If responding beyond the area of hostilities, you want to ensure that you’re not stepping on other legal boundaries.

Textual Description Summary for Participant #14 (DS240017)

Participant #14 described the experience of decision-making uncertainty following a cyber attack based on the complex relationship between the current legal framework and existing policies governing response authority. “I do think that the authority issues are not as complicated as people think that they are. I think that the authorities and what one can do are reasonably clear. However, what’s less clear is what exactly people want to do. So, what we want to do is less certain. The authorities a little bit more clear. Then when people run into the answer of we don’t have authority to get you to where you want to be, then the road to acquiring new authorities works through the interagency, up through congress, and up through the president. That process has a

life of its own. So, responding is a policy matter, because the policy has to be answered as to how and where we're going to operate in certain domains. Then once that decision is made, the authorities will be written to support that policy matter."

Participant #14 also identified cyber attack recognition, context, and analysis are complex and influence decision-making uncertainty. "I think it boils down that responding in cyberspace is complicated . . . this is a complex environment and it's very difficult from the macro level to decide in a very linear fashion where the red lines are. So, in that calculus, to come with a legal answer we have to know what the anticipated benefits are, what the anticipated costs are. I think that there's levels of skepticism that exist for the capability and the ability to control and minimize damage. But, those are technical things." Participant #14 added, "The ability to defend ourselves or operate in this environment gets complicated, but I think that is due to the absence of national level guidance and having it trickle down. We need a leader to say, 'This is how we're going to do things. These are the roles I want the agencies to play.' In this context, what are the rules that govern individual circumstances and who is in charge when conducting cyber responses?"

Textual Description Summary for Participant #15 (DS240018)

Participant #15 described the experience of decision-making uncertainty following a cyber attack from the perspective that the existing legal framework is inadequate to support complex response options given the existing capabilities. "Absolutely, we lack a clear legal framework. You can see it. Choices should be made at the lower levels based on regulations and policies. But, at the DOD level, decisions are not made at the lowest level because the lawyers get involved. And, although actions

need to be taken, much decisional uncertainty exists. I think there are challenges to have a simple single decision-maker, partially because of the U.S. government design. Because of how we structured the executive branch and . . . the blurred lines between departments and agencies, the response process becomes overly complex. I think we're growing . . . training and execution capacity, including the legal authorities. But, the response options are so complicated that I don't think in my lifetime – not my career, but my lifetime, that it will be an effective tool for us.”

Participant #15 also considered that existing military and generational culture factors influence decision-making uncertainty and response processes. “Just by the nature of command and control of the military, I think creates a weird balance, complicated by the fact that even today senior Generals and Admirals didn't grow up with computers. It was introduced as they were in college or Lieutenants for the most part, whereas junior officers today have much more experience. From a senior officer's perspective, they want to use the right weapon for the right application. However, in cyberspace, they're not sure what that is yet. Senior officers have a different perspective due simply to not knowing what is at their disposal. We have kept it so classified for so long that their broad knowledge base is, ‘Well, let's hack that. Let's do a denial of service. Let's do spear fishing.’ Their training and their experiences have not brought them up to make these choices. Whereas, they can see a gun, a ship, a tank, an aircraft, or bomb, they cannot see cyber weapons.”

Textual Description Summary for Participant #16 (DS240019)

Participant #16 described the experience of decision-making uncertainty following a cyber attack based on the lack of national policy and a comprehensive

strategy resulting primarily from ineffective collaboration between interagency stakeholders. “The policies are lacking. There really isn’t a uniform opinion or policy across the U.S. government on cyberspace and what is allowed by the different departments and agencies and what is generally considered operating norms internationally. And, there’s certain dynamics in play in which I think certain agencies in the U.S. government want to keep those walls up. Although there are policies in place that govern the use of cyberspace, there’s nobody in the U.S. government right now thinking about a cyber shockwave scenario. You have many U.S. government agencies that are very good at their ‘siloed’ mission in cyberspace, but when it comes to the integration of everything to address a specific issue, they failed. And, we will fail . . . unless we integrate existing concepts, policies, and missions to defend the nation against cyber attacks. There must be uniform agreement on that.”

Participant #16 added, “I’ll give you an example. There’s an open source news story concerning certain nation states that have been found in our electrical grid networks. The story’s author asked, ‘What reason would a nation state be inside our electrical grids or our industrial control systems? What reasons other than operational preparation for war since electrical grid networks have no espionage value to a nation state?’ So, if you take it to the next step, well, if they are preparing for war and if they do finally execute these kinds of things, we should be able to respond with the use of force with the full power of the United States military. Therefore, we should have some sort of deterrence policy first, some strategy that tells the world we don’t stand for this; if we find you conducting these kinds of activities, we will respond with force.”

Participant #16 also conveyed that decision-making uncertainty is influenced by the concern to use existing cyber capabilities during integrated operations as traditional military activities. “Given the existing legal framework, from my perspective, the current authorities, legal authorities to conduct cyberspace operations on a global scale are inadequate. When dealing with the authorities to conduct cyberspace operations outside of areas of hostility, very complex legal impediments result. There are few things in play here such as the legal ramifications of conducting operations in sovereign countries on commercial servers . . . where Internet service providers are bound by commercial property laws and sovereignty, privacy rights, and civil liberty concerns. Participant #16 further noted, “There are different ways of thinking about cyberspace because of the intelligence community’s culture. They don’t think of it as a warfare domain, but as a means of conducting [intelligence gathering] operations to obtain information using sophisticated tools and techniques. But, they don’t see it as warfare; they see it as more like espionage.”

Textual Description Summary for Participant #17 (DS240020)

Participant #17 described the experience of decision-making uncertainty following a cyber attack based on the need for enhanced understanding of existing capabilities and improved technology utilization. “I think a new level of understanding can evolve, but I think from a military perspective, we haven’t figured out how to share knowledge effectively. I believe we need to look at the way we teach our special forces to use cyber capabilities because this domain is all about being adaptable. The technology life cycle must improve. R&D cannot be a five-year procurement process. Technology being developed today needs to be in the fleet and in the field six months

from now.” Participant #17 also expressed, “Coalition forces have to be able to attack a network or attack nodes on a network. So they have to understand how the traffic moves and where does it reside, including the best place to intercept it, stop it, or to jam it. Because that’s a virtual concept, you have to figure out what would that look like in the physical world.”

In addition, Participant #17 noted that ineffective training curricula, technology overexposure, and a generational divide influence decision-making uncertainty. “I think that generational differences affect the ability to respond to cyber attacks. Based on my training command experience, I saw a whole bunch of 18-year olds rolling in. There are a couple of thoughts here. One, part of it has to do with the generation. The Millennials come in really dedicated and motivated to do something for their country and they were comfortable with the technology. Now, with that said, they were not comfortable with learning on the technology, if that makes sense. So computer-based training, they weren’t taught on computers in primary school, so rolling into an area where you’re supposed to learn an entire career field on a computer using a computer-based training program doesn’t necessarily work because that’s not how they learn. But, they are very comfortable experimenting with technology and will be out there - way ahead from an innovative perspective regarding cyber warfare.”

Textual Description Summary for Participant #18 (DS240021)

Participant #18 described the experience of decision-making uncertainty following a cyber attack from the perspective that the absence of national policy, an inadequate legal framework, and the lack of familiarization with existing capabilities reduce response effectiveness. “I think we lack clarity and familiarization with concepts.

If folks were up on concepts and capabilities of what they can and cannot do, I think we would move closer to developing a national policy, a whole of government strategy on how we approach cyber warfare decisions. We certainly don't have a government strategy, even though we've had a national plan [Comprehensive National Cyberspace Initiative]. We've had a number of government studies on it. I also think the legal frameworks are inadequate. I think we have a recognized need out there, but I think we have ambiguity, extensive ambiguity, in policy, in doctrine, and the law. Certainly, we're moving towards formalizing doctrine on cyber policy. But, all of the disparate studies only contribute to the confusion that commanders face as to what it is we can do and can't do in cyberspace."

Participant #18 also described how cyber warfare characteristics influence decision-making uncertainty based on the challenge of deterring a myriad of actors and the need to protect the nation's critical infrastructure. "We're concerned about potential adversaries, potential peer adversaries, bad guys out there, and not just nation-state actors, taking advantage of potential vulnerabilities or capabilities. That ambiguity, I think, works in our favor in the absence of clear policy or frameworks. International, for example, we don't have clear rules of the road, code of conduct for cyberspace. We don't have international laws, rules of behavior, which everybody signs up to. We don't have those things at a national level, so that uncertainty about capabilities is a constraining effect, I think, on some of the actors. Unfortunately, because of the multiplicity of actors, plausible deniability by working through cut outs, of using botnets, of harnessing huge amounts of botnets right now, like certain malware out there does, it's really impossible to know who's doing the damage."

Participant #18 added, “We don’t have consensus on how we approach this domain that has become so critical, so vital, to our national survival, to our national fabric – our financial institutions, banking institutions, SCADA systems. Everything is tied to cyber, and not just here in this country, but increasingly globally. We don’t have yet in our own minds sorted out, for example, what is sovereignty in cyberspace? The fundamental concept of international relations, such as sovereignty, does that apply in cyberspace? It must get sorted out, because I think in many cases, commanders just choose, because of that ambiguity, other than net operations, they choose to ignore cyber or to bunt it or to say we’re going to focus on traditional warfighting means and cyber is an adjunct. Cyber is an enabler, rather than a warfighting domain that we need to be cognizant of in and of itself, similar to strategic communication or similar to IO.

Textual Description Summary for Participant #19 (DS240022)

Participant #19 described the experience of decision-making uncertainty following a cyber attack based on understanding the tension between cyber operations being considered intelligence gathering versus traditional military activity. “We obviously know we haven’t figured out all the legal issues of dealing with cyberspace, whether it’s Title 10, Title 50 intelligence collection, where the military line is versus the intelligence line versus the open dialogue of use of the Internet versus disruption. I mean, we don’t know. It’s very murky right now in terms of the legal definitions. We have – certain authorities have been grant to us, approved by the president to do certain things with legal oversight, obviously, and limits, but we don’t have enough operational experience to really understand whether it’s sufficient or not. In addition, you’ve got the Department of Justice trying to understand basic traditional military activity as it pertains

to cyberspace, so if they're wrestling with writing opinions on that, you can imagine the legal sufficiency to do certain things in cyberspace is immature.

Participant #19 also conveyed that decision-making uncertainty is influenced by inconsistent rules and regulations and the lack of declaratory policies, which limit our ability to respond to cyber attacks against critical infrastructure. "I think there has to be a balance. I mean, whatever we believe to be true, we would want our adversary to believe the same, so there has to be rules. I mean, if we live by a set of rules and then other nations live by the 'Wild Wild West,' well now, we have a different framework. I believe there has to be rules to conduct business and warfare in this seemingly ungoverned space. To a degree, a national policy would be similar to a gun law. I think most of it though is that we don't want to box ourselves in with a declaratory statement or a policy that we would have to hold ourselves to. However, until you declare what those lines are, gaining access to our critical infrastructure remains likely with inevitable attacks detrimental to the integrity of the nation's SCADA systems and banking sector.

Textual Description Summary for Participant #20 (DS240023)

Participant #20 described the experience of decision-making uncertainty following a cyber attack based on the perception that interagency leaders require improved collaboration and understanding of cyber warfare characteristics. "I think there's two ethical aspects to consider. One is the perception, right or wrong, and I think it's very situation dependent, that cyber weapons are not well controlled. It's hard to ensure proportionality, discrimination, and so forth if you're not absolutely certain that whatever you do won't escape into the 'wild' and propagate through the networks. It's hard to demonstrate that you have that kind of control because just by the nature of the

weapon and that maybe people can't abide by the laws of war in cyberspace. Two, I think the only other ethical issue is property based. The DoD, unlike the State Department or the CIA, tends to look at cyberspace as borderless, non-geographic, not very closely related to private property. It sees private property as just a transit point for activity."

Participant #20 added, "There's work being done on the legal and policy issues by an interagency group from Department of Justice, Department of Defense, Department of Homeland Security, Department of State, and Treasury to refine what constitutes the use of force in cyberspace since we use that to justify use of force responses. The Department of Justice is also ruling on the legality of different types of cyber operations, who has what authorities in the interagency to conduct what types of operations, and under what conditions. I don't think we devoted sufficient resources to developing a national policy in the sense that it just hasn't become a priority yet. Neither do I really think that there's been a concerted effort to not define it. I think every agency is working very hard to define it in their agency's interests, but there's been no crisis to force a melding of the minds. I would like to think that that a catastrophic cyber event is not necessary, but, nothing in my experience suggests we're going to come to a consensus without something like that."

Participant #20 also expressed that decision-making uncertainly is dependent on the acceptance that cyber operations are traditional military activities. "I think there are traditional military activities to be conducted in cyberspace. That's not quite the same thing as saying that cyberspace operations are inclusively, across the board, all of them, a traditional military activity. You can do many things in cyberspace. Some are traditional

military activities; some are not. But, there are many military activities that have analogues in cyberspace, and where analogues exist, they should be treated as traditional directives. Participant #20 further noted, “People think that cyber operations are a form of *fires*, fires are under the control of combat commander. Combat commanders should have control of their fires like every other kind of fires, or we will never integrate it effectively into joint war fighting. I personally think you can integrate it effectively into joint war fighting in the same way that we integrate global transit with centralized command and control that services the needs of the combat commanders.”

Textual Description Summary for Participant #21 (DS240024)

Participant #21 described the experience of decision-making uncertainty following a cyber attack based on the need for improved understanding of existing capabilities and response options. Participant #21 also discussed concerns that the current legal framework and policy void prevent the effective integration of cyber warfare into normalized decision-making processes. “I think that cyberspace operations are still nascent enough that legal discussions are now just maturing to a point where we understand there is inadequate policy there. I think the topic is so complex, one, people are afraid to try to get their arms around it until they’re forced to, and two, only then do they realize the complexity of doing anything in cyberspace. Because everything’s connected, the ramifications of action or inaction present a broad range of things that you need to consider. They’re tough things to consider, and making decisions, certainly as policy makers, is hard because making a bad policy decision in cyberspace can have many unintended side effects.”

Participant #21 continued, “I think the lack of policy is at a national level, primarily. If you, as a nation, prescribe to one thing or another, that decision sets the tone all the way down. If you choose not to set that tone, there’s much ambiguity below that leaders can’t make a command decision; I must now make a legal decision based on the lack of a policy directive. With respect to response capabilities and options, Participant #21 asserted, “I think if you want to stick with the current construct of combatant commanders in charge of regions of the globe, and functional commanders in charge of domains, you are going to need decentralized authorities and decentralized executions. That’s not to say you won’t need standards so you can develop levels of situational awareness, but I think a combatant commander, because he’s been tasked by the president to achieve something, needs to own the ability to shape and control his networks and use cyber tools as part of his plan.”

Participant #21 expressed concerns that decision-making uncertainty is influenced by the reluctance to integrate cyber warfare into normal operations. “I would say right now, the number one thing that we wrestle with every day no matter what the operation is, particularly with the intelligence community, is the discussion over intelligence gain/loss and operational gain. Historically, the intelligence community has won all disagreements based on the argument that the intelligence loss is just too great. In my opinion, we have not fully integrated cyberspace into operational planning. The mindset of the people who do strategic and operational planning have failed to synchronize all those lines of effort and lines of operation by including cyberspace into the strategic end state. It is only recently that we’ve started to wrestle with cyberspace operations, asking

how does that support not only kinetic operations, and all the other things that we do, from network operations to attack. How is all woven together?"

Appendix M: Individual Structural Descriptions

Individual Structural Descriptions

The individual structural descriptions capture the participants' deep and underlying feelings, reflections, and emotions associated with the decision-making uncertainty they experience when determining the appropriate response following a cyber attack. The structural descriptions were constructed from the individual textual descriptions and key themes by employing imaginative variation, reflection, and analysis. The structural descriptions provide an account of the underlying dynamics of "how" senior military officers experience uncertainty when making cyber attack response decisions (Moustakas, 1994).

Structural Description Summary for Participant #1 (DS240004)

Participant #1's experiences were founded on 21 years of Navy service and a Joint Staff strategic policy background. Participant #1 believed "the legal construct and its interpretation require certain organizations in our government to consider any operation greater than network defense to be covert, and controlled by that organization, which clearly limits our traditional military activity response." Participant #1 shared, "I believe a cyber attack in my mind carries with it the same weight that allows a response under the standing rules of engagement without getting permission from anyone other than considering your inherent right to self-defense." Participant #1 did not feel required to respond in kind to a cyber attack. "I feel just because someone attacks us in cyber world doesn't mean we have to attack the same way, I think there's other different ways you can respond to a cyber attack. It doesn't have to be with a cyber attack." In addition, Participant #1 perceived, "Most military leaders are not trained and do not understand cyber warfare or anything about cyber capabilities."

Structural Description Summary for Participant #2 (DS240005)

Participant #2's experiences were founded on 22 years of Marine Corps service, over 20 years of commercial information technology employment, and a Joint Staff strategic policy background. Participant #2 stated, "Regarding the use of force, I would not ask the question what a cyber attack means. In my mind, the issue is not what it means. It's really what is a cyber attack? Give me the words, I'm looking for the words that describe what it is for me." Participant #2 felt, "It's a semantics argument, a definitional problem, that I perceive exists because the use of term cyber attack has such a large variance of meanings that it's almost useless in its existing construct unless we can nail it down a little bit more for commanders to make decisions against without so much ambiguity. To Participant #2, responding to a cyber attack is dependent on intent, capability, and resolve. "To show a hostile intent in cyberspace requires ability and will." Further, I feel "responding requires the authority in place, which permits the use of force."

Structural Description Summary for Participant #3 (DS240006)

Participant #3's experiences were founded on 28 years of Air Force service and a Joint Staff strategic policy background. Participant #3 believed, "The most knowledgeable entities that we have are probably the intelligence community who have a presence in cyberspace for appropriate, legitimate, and valuable reasons from intelligence channels to the technical channels. This contributes to the uncertainty and establishment of a policy presence at the operational and tactical level." Participant #3 felt, "Obviously, there are turf issues and people feel like there's ownership of what's mine and where the resources are aligned, but I think people could see beyond that if we had an overarching

policy that would focus what we're trying to do, what's all right to do, and what's approved to do." Participant #3 perceived, "I believe we need to come to grips with the notion of privacy versus anonymity, especially as it pertains to cyberspace. It's very difficult to deter when the actors could be everyone from an individual to a non-state actor to a nation state and so the 'who' factors in greatly in deterrence."

Structural Description Summary for Participant #4 (DS240007)

Participant #4's experiences were founded on 16 years of Air Force service, over 14 years of military information technology training, and a Joint Staff IO background. Participant #4 stated, "My number one belief is a lack of respect for the technology. I don't think that senior leaders understand how difficult it is to develop the technology that looks like a commodity. For example, the Blackberry, they have no idea of the complexities and the design and the technical wonderment that goes into making that device new and improved every year. And, how many billions of dollars and thousands of people that Motorola puts into that one device even, as an example. So I used to call it a respect, I just don't think they have an understanding of the complexity which we deal with." Participant #4 also had feelings about the virtual duality of cyberspace. "I think that we get into this concept of your private information really is you. People think that if something is done with that information, that virtual representation, that they actually kill you.

Participant #4 shared, "So this concept of identity theft, when somebody steals your credit card and your ID, people say that that's your 'true' identity. Well, when I grew up, your identity was wrapped up in your character, things deep inside of your heart that nobody could ever take from you. Now, we have made it a digitized form and

people can steal it from you, and I think that that's cataclysmic to them, that the idea that they could lose their identity. So, I think that there's a hypersensitivity to understanding what's virtual versus what's real." Participant #4 had strong beliefs regarding reversibility of cyber attacks. "Literally, I can't think of anything in cyberspace that would not be reversible at some point. In kinetic warfare, I can't undo the effects of a weapon once it detonates, I can't reverse that. But, in cyberspace, almost any action or effect is reversible. If it's reversible – well, I didn't really take down the stock exchange, just making you think I could is the effect."

Structural Description Summary for Participant #5 (DS240008)

Participant #5's experiences were founded on 17 years of Air Force service, over 15 years of military information technology training, and a Joint Staff strategic policy background. Participant #5 felt, "Senior leaders who are in the position to make decisions on the application of force in response to a cyber attack are not familiar with activities in the domain. They are not comfortable with them. There's a layer of complexity there." Participant #5 had strong feeling about the decision-making process from a military perspective. "Even when made aware that a response option is made available to them, the command and control is not clean, and they're not sure who gives the authority, who has categorized this attack in the right way." Participant #5 expressed his beliefs regarding hostile acts in cyberspace. "We're framing attacks in cyberspace in the same lens that we do physical attacks, and we are trying to model standard rules of engagement in cyberspace based on standard rules of engagement that we have in the physical world."

Structural Description Summary for Participant #6 (DS240009)

Participant #6's experiences were founded on 14 years of Navy service and a Joint Staff strategic policy background. Participant #6 approached the lead interview question by comparing a cyber attack to an equivalent kinetic attack. "Did an attack occur or was this just some sort of accident? If you compare a cyber attack to a traditional attack, such as a bomb or a terrorist attack, I think there is a lot more uncertainty in what I call *discovery*. Because we have malware, computer glitches, and ghosts in the machine, there's generally a longer period of discovery for a cyber attack than a kinetic attack. That's definitely one of the uncertainty factors that quickly come to mind. Participant #6 was concerned with what constitutes a use of force in cyberspace. Participant #6 felt, "Understanding the definition of 'use of force' or 'act of war' is an uncertainty factor that would impede your ability to decide if a use of force is needed. Interwoven into this uncertainty factor is the need to define the line between criminal activity and warfare."

Structural Description Summary for Participant #7 (DS240010)

Participant #7's experiences were founded on 26 years of Air Force service, over 25 years of military information technology training, and a Joint Staff network operations and strategic policy background. Participant #7 beliefs became evident through the shared perceptions regarding the different Service cultures. "You have just different methods to how each Service of the military approaches cyber warfare. You have the Army as a very tactically focused type of Service, so in their culture, their viewpoint of cyber warfare is probably at the tactical edge, and they're out there working and doing things at the point of the spear. The Air Force looks at it more corporately, and they're

not necessarily out there at the pointy end, forward in theater, but they approach things from more centralized perspective. And, you have the Navy's construct of being deployed at sea, so their perspective is based on mobility. And, there's Marines, I think they have a self-sufficient, decentralized point of view. Regardless, I think you absolutely have significant cultural differences on how to approach cyber warfare."

Structural Description Summary for Participant #8 (DS240011)

Participant #8's experiences were founded on 19 years of Navy service, a Joint Staff legal and policy background, and substantial postgraduate work in cyber law. Participant #8's beliefs and values were heavily influenced by a legal perspective. "First and foremost with respect to the decision-making process, when deciding how to respond to a cyber attack, the decision-makers utilize the same criteria, or should use the same criteria. You need physical evidence of where the attack originated, and generally, that leads you, rapidly, to an answer as to who caused the attack, so you know from an identification standpoint, who you can respond against. The biggest difficulty with cyber attacks is the difficulty in ascertaining and positively identifying the source of the attack. Participant #8 firmly believed, "It's not a question of the legal framework's adequacy, but there are policy decisions that need to be made with respect to thresholds that define when commanders can respond. Remember, the Commander-in-Chief has the prerogative to limit the application of any formulation of military policy or policy with respect to the use of force."

Structural Description Summary for Participant #9 (DS240012)

Participant #9's experiences were founded on 21 years of Air Force service and a Joint Staff force structure and resourcing background. Participant #9 believed responding

in cyberspace is a function of making judgments about perceived hostilities and the effects of the attack. “Any threats or perceived threats toward the United States or our allies that result in a negative economic, political, or social impact are things that, I think, we would respond to. If attacked along those three lines, I believe our leaders would have a hard time trying to differentiate or caring about the method. Therefore, if it impacts these areas, we will act with a proportional response, whether it’s cyber or conventional based on its effects. When you look at cyber, the immediate impact may not be apparent. You may not realize what the impact is for several months, for a year, maybe more, whereas when you bomb a shelter, or bomb a village, or whatever the case is, there’s an immediate effect at the social, political, and economic levels. Therefore, cyber war is effects-based.”

Structural Description Summary for Participant #10 (DS240013)

Participant #10’s experiences were founded on 16 years of Air Force service, over 15 years of military information technology training, and a Joint Staff network operations and strategic policy background. Participant #10 had strong contextual perspectives and beliefs. “I think cyber warfare is very contextual. In fairness, I think kinetic attack responses are contextual as well. There has to be some thought and logic applied. You have to avoid the objective black and white response, ‘Well they dropped a bomb, and we drop a bomb.’ Cyberspace complicates that decision process further. The concept of response thresholds must be seriously considered. For example, consider a dam being attacked. If the dam was taken out in the United States and it flooded a couple of cities, that’s obvious. But, if the dam was stopped and just caused a couple of power outages for a couple of hours, that’s different. So, I think there’s a lot of context that has to be

applied. Determining a proportional response is much more than blindly adhering to black and white rules.”

Structural Description Summary for Participant #11 (DS240014)

Participant #11’s experiences were founded on 27 years of Marine Corps service and a Joint Staff IO background. Participant #11 described decision-making uncertainty from the belief that warfare responses are intrinsically coupled to identifying the attacker. “Fundamentally, uncertainty comes down to the inability to positively identify your target from a kinetic sense, a source of where the fires [attacks] are coming from. Is the fire coming from inside a house, from a mosque, from a church, from a school, an otherwise protected sanctuary has crossed the line and can be positively identified as the source of the attack? Cyberspace not only is the source of the target, or the source of the attack, but also provides a difficult if not impossible safe haven to identify. Cyber attacks can be disguised; can provide misperception; can come from an indirect approach; and can come from within. It’s an unbelievable challenge and every time we talk about the hostile acts going on right now; in my mind, it doesn’t provide any more clarity. I believe that’s the fundamental difficulty, identification of the target.

Structural Description Summary for Participant #12 (DS240015)

Participant #12’s experiences were founded on 14 years of Navy service and a Joint Staff strategic policy background. Participant #12 believed organizational and national responsibility to be essential when responding to a cyber attack. “First and foremost is attributing the source of the attack. Where did it come from? Where do we think it came from? And, what degree of certainty to do we have? I think that the degree of certainty is important. Because even if unable to determine down to the individual

level, you can probably determine down to a geographic area as far as the point of origin of the attack. And, much like we have approached in the war on terror and the counter-terrorism environment, we place a certain amount of responsibility on nations. And, within their sovereign right, if attacks are organized, trained, planned, or executed via a sovereign country the international community holds a certain degree of responsibility to the nation that is the host, whether knowing or unknowing, to the source of the attack.”

Structural Description Summary for Participant #13 (DS240016)

Participant #13’s experiences were founded on 23 years of Army service, over 20 years of military information technology training, and a Joint Staff strategic policy background. Participant #13 viewed the decision- process of responding to a cyber attack from a warfighter’s perspective based on evaluating unintended effects. “So when you’re looking at responding . . . I mean you really have to look at it as a commander on the battlefield. Because warfare itself has its own degree of uncertainty, am I willing to respond if my actions have small or low collateral effects? Yeah, I think I would. I could live with low collateral effects. But, it really depends upon where the collateral effects occur, or you know, what damage they cause. Certainly, within my area of responsibility, I have to evaluate the collateral effects and determine if I can stomach the unintended consequences. However, if I go beyond my area of hostilities, I’m going into other areas, other countries, I would be a more concerned to ensure that I am not causing cascading effects or violating international laws.

Structural Description Summary for Participant #14 (DS240017)

Participant #14’s experiences were founded on 17 years of Army service and a Joint Staff legal and policy background. Participant #14 described decision-making

uncertainty from a heavily influenced legal perspective with emphasis on the laws of armed conflict. “I think that operators want lawyers to tell them what they’re allowed to do to shape the operation. Whereas, lawyers need facts in which to render an opinion. So, the lawyers have to say, ‘Tell me what you want to do so I can figure out does your contemplative action fit within the left and right parameters of the authorities that exist.’ Therefore, the balance between operators and lawyers don’t always mesh well. I think that the law is not as complicated as people want to make it sound.”

Participant #14 added, “In order for a nation to conduct a military operation, there has to be a military necessity for it. And then when you’re weighing the cost and benefit of a military operation, you have to look at the desired objective that would be achieved, the military gain, against the collateral damage, meaning the damage that occurs to people, institutions, property, whatever that is beyond just the effect that you’re trying to achieve. ‘Civilian collateral damage’ is a simple way of saying it. For the response process to work in cyberspace, operators and lawyers must collaborate. That’s where the lawyers say to the operators, ‘You want to know do you have authority to do this? Well, what is it that you want to do? Give us the detailed facts.’ When we have the facts, we can begin to marry up the detail operation that’s planned against the required authorities.”

Structural Description Summary for Participant #15 (DS240018)

Participant #15’s experiences were founded on 20 years of Air Force service, over 18 years of military information technology training, and a Joint Staff network operations background. Participant #15’s beliefs were shaped by extensive postgraduate work conducted on understanding United States and international law and policy regarding information warfare. “The lines of responsibility and authority are complicated in the

cyber arena. Unlike 100 years ago, 200 years ago, where a buildup to war was typically over a more significant timeline, where you had the opportunity for debate, discussion, who did it, why they did it – cyber warfare occurs at network speeds. The timeline shrank considerably when cyber weapons became a reality. So, we have to make some policy and supporting legal changes to respond effectively to cyber attacks. We have to stand up processes internal for the government to deal with that. We have to develop a much more rapid, cleaner line of authority. Because we are talking about using cyber weapons, these changes are the responsibility of the Department of Defense. Once the policies are clearer, the response decisions are easier.”

Structural Description Summary for Participant #16 (DS240019)

Participant #16’s experiences were founded on 21 years of Air Force service, over 20 years of military information technology training, and a Joint Staff network operations and policy background. Participant #16’s perspectives were centered on understanding how sovereignty, privacy, and civil liberties influence decision-making uncertainty. “The concept of sovereignty is complex due to the global nature of cyberspace. These complexities add uncertainty to the decision-making process. There are privacy rights and civil liberty groups as well as the Department of State (a real big proponent of this) in the U.S. government right now discussion the concept of sovereignty in cyberspace. These groups are trying to understand the legal, policy, and property right issues governing how where data resides, who owns data, who owns data in transit, and also who owns the information technology when data is [sic] transiting. These issues come into play on ownership and sovereignty when making decision to respond to a cyber attack. The policies concerning sovereignty are lacking. There really isn’t a uniform

opinion or policy across the U.S. government on the sovereign nature of the cyberspace domain.”

Structural Description Summary for Participant #17 (DS240020)

Participant #17’s experiences were founded on 24 years of Navy service, over 22 years of military information technology training, and a Joint Staff network operations and policy background. Participant #17’s beliefs and insights were shaped predominately by extensive signal intelligence and cyber warfare educator experience. “We’re always behind with respect to education and training efforts. I mean we should put in a ‘warfare center,’ a cyber warfare center for training. However, we just don’t invest that much money and energy into our training. There are lots of reasons to do that, such as allowing students to grow and become adaptable with cyber tools and capabilities based on their experience with software programs like World of Warcraft. We have the technology to create an Afghanistan environmental simulation in our own home, so why don’t we do that in our training environment? The R&D of that simulator is not that difficult. However, cyber simulators are not built due to the existing policy to develop multi-purpose simulators . . . for pilots, navigators, and maintenance training. We don’t allocate the money and resources to improve cyber warfare training programs.”

Structural Description Summary for Participant #18 (DS240021)

Participant #18’s experiences were founded on 31 years of Army service and a Joint Staff strategic policy background. Participant #18’s perceptions and views relied heavily on foreign diplomatic service experience. “We don’t have a clear way ahead on how we would accomplish certain military activities, which would have certain effects in cyberspace. We need a government, a whole of government template for that because,

again, the DoD can't do anything here in exclusion. The synchronization, as you well know, for conducting sensitive operations in cyberspace is too complex without that level of collaboration. And, because of the collateral effects that you're going to have because of cascading events that you have in cyber – unforeseen, unpredictable events – you need to have consensus. Therefore, before the DoD does anything on its own, everything has got to get trotted out by the National Security staff to ensure interagency collaboration, so that everyone at least has cognizance of the initiatives, policy changes, and planned operations. Response decisions along with the potential higher order effects must be explained to make sure that we [DoD] don't step on our interagency partners' equities.”

Structural Description Summary for Participant #19 (DS240022)

Participant #19's experiences were founded on 26 years of Navy service and a Joint Staff IO background. Participant #19's beliefs and values were framed by the perceived importance of understanding authority, chain of command, and organizational responsibilities. “The command and control construct is important in terms of normalizing cyber warfare. We must recognize that in certain areas it has to be centralized, in certain areas it needs to be decentralized, so I think it's a mix and dependent on the situation. As we mature in this domain, we must develop thought processes designed to normalized cyber with other military operations. I think we have to find that balance. I mean, in the Navy, as you know, we have command by negation, which is important to us because sometimes you have to decentralize and delegate authority to properly defend yourself or to take immediate action. But in some cases, it has to be centralized for lots of very important reasons such as coordinated and synchronized operations. I think there's a balance.”

Structural Description Summary for Participant #20 (DS240023)

Participant #20's experiences were founded on 20 years of Air Force service, over 18 years of military information technology training, and a Joint Staff IO background. Participant #20 approached the phenomenon of decision-making uncertainty by recognizing the importance of roles, responsibilities, and declaratory policies. "I think cyber deterrence requires a national declaratory policy. Whether or not it works remains to be seen, but I think, as a nation, we have to try. How can you not try? As reliant as we are on cyberspace, how can you not do whatever you can to try to deter malicious activity? This requires us to define what our role as a nation is going to be.

Participant #20 shared, "In cyberspace, we need to establish the broadest set of response conditions so if someone attacks our civilian infrastructure, we're can strike back. There's been so much discussion about our hands being tied by attribution and we'll never react, but the reality is, like with 9/11, if you hit us hard enough, we're going to hit back. I believe making it clear that certain soft underbelly targets that are not military, such as financial, power grid, emergency response, disaster recovery, and those kinds of functions are absolutely off limits."

Structural Description Summary for Participant #21 (DS240024)

Participant #21's experiences were founded on 18 years of Marine Corps service and a Joint Staff IO background. Participant #21 shared beliefs and perspectives regarding the leadership qualities and characteristics necessary to be an effective cyber warrior. "I think my first inclination is to say a warfighter in cyberspace absolutely needs to be a guy trained in the career field, just like space operators. However, the second I think through it, I pull back to realize that cyberspace is so unique and tied to so many

other systems that it might need to be a person with a number of specialized skills, yet with traditional military experience as well. For example, a cyber person might work at a computer his entire career, and grow up to command a unit with wartime cyber capabilities.”

However, Participant #21 expressed, “He may understand exactly what those technical capabilities can do, but he still must have the experience of living on the other end of the warfighting spectrum in order to understand or interpret what a commander is asking for. He needs to understand how cyber effects might be delivered, the political, and the legal ramifications that can only be developed over some years of indoctrination. However, I don’t think you can, in cyberspace, hold out for a person that is a purely cyber warrior. From a DoD perspective, we need to figure out how to shoot, move, and maneuver in cyberspace. In that sense, it’s no different than land warfare or combat on the high seas with ships of the line. It is engagement; it’s very much an art of war. The art piece of it requires years of cyberspace indoctrination in order to apply those skills effectively to conventional conflict.”

Appendix N: Composite Textual and Structural Descriptions

Composite Textual and Structural Descriptions

Composite descriptions enhance understanding of the participants' perceptions and lived experiences by constructing a comprehensive representation of the group as a whole. Composite descriptions are constructed from the individual textual and structural descriptions. Keen (1975) noted, "It is not possible to describe texture without implicit notions of structure" (p. 58) due to the inherent relationship between texture and structure. Therefore, composite descriptions provide a contextual and holistic construction of perspectives for understanding the meanings and essences of the experienced phenomenon.

Textual Composite Description

The textual composite description was developed from the individual textual descriptions by integrating the invariant constituents and key themes to depict the experiences of the group as a whole. Focusing on the textual qualities of the experience provides a better understanding of the supporting meanings behind *what* was experienced. The textual composite description is presented by key theme in order to reveal what the senior military officers, as a group, perceived when experiencing decision-making uncertainty following a cyber attack.

Response Characteristics and Efficacy Considerations

An overwhelming number of participants described the experience of decision-making uncertainty following a cyber attack by emphasizing the lack of response options at their disposal. They expounded on this perception by describing how the lack of defined response thresholds ("red lines") prevents the determination of *necessity* (i.e., legitimate need) to respond in accordance with the laws of armed conflict. Because

response thresholds (“lines in the sand of warfare”) are not properly defined, the participants described the decision-making process as unresponsive, untimely, and ineffective. Most participants shared that responding to an attack in cyberspace has the added complexity of *proportionality* due to the inability to determine contextual equivalence of the attack in terms of traditional warfare.

The majority of participants described the response process to be impeded by ambiguous lines of authority at the operational level. Further, most conveyed responding to attacks in cyberspace to be complicated by technical challenges associated with cyber target discrimination and *distinction* (i.e., the ability to differentiate accurately valid military targets from civilian or non-combatant targets). Several participants stated that response options lack scalability, which reduces the options of responding effectively to the large range of cyber attack severities encountered. For a few participants, developing and incorporating better autonomous response capabilities that adequately address less severe cyber attacks, which occur more frequently, would minimize decision-making uncertainty.

Social, Behavioral, Cultural, and Cognitive Aspects

All participants described the need for an improved level of individual understanding regarding the complex dynamics, interrelated effects, and decision-making processes associated with cyber warfare. Most participants expressed that their inadequate level of understanding was limited by the lack of a common lexicon and an inconsistent vernacular, both of which are exacerbated by diverse values and belief systems from the numerous stakeholders with equities in cyberspace. Further, some

participants added that their insufficient knowledge level negatively affected their self-confidence and ability to make sound decisions as a cyber warrior.

Essentially every participant explained that generational differences (i.e., cultural and ideological variances resulting from differences in age) added to the decision-making uncertainty associated with responding to a cyber attack. Admirals and Generals (Baby Boomers) view cyberspace much differently than Lieutenants (Millennials). Most participants also noted that the differences between the military and society's view of cyberspace affected their response decisions. From their perspective, the military views cyberspace as an operational domain of business and warfare, whereas society views cyberspace as a social network medium for collaborating and communicating. Several participants further highlighted that the differences in academic (free exchange of ideas) and commercial (ideas exchanged for profit) cultures appreciably affected their decision-making uncertainty.

When expressing their thoughts regarding the social nature of cyberspace, several participants indicated that the existing international norms of behavior influence their decision-making process based on what is perceived as the acceptable bounds of response options. These considerations were noted by several participants to affect large policy decisions such as deterrence and response thresholds. Many participants conveyed that *dehumanizing* cyber warfare would lessen the uncertainty of making challenging response decisions. By relegating cyber warfare to machine versus machine, the participants asserted the proper perspective is achieved regarding the detrimental effects of the response.

Policy and Strategic Aspects

Nearly every participant had a perception that decision-making uncertainty is influenced strongly by an inadequate national strategic policy regarding cyber warfare. These participants asserted the lack of national policy limits the leadership's consideration of using cyberpower as a legitimate instrument of national power. Considerably adding to the level of uncertainty, most participants conveyed that the relative level of attribution required to respond to a cyber attack was arbitrary and unrealistic. The participants added that the technical challenges associated with achieving a high degree of attribution confidence governs the desire to establish and declare deterrent consequences. Most participants explained that the inability to develop an effective cyber deterrence policy is compounded by the sheer number of actors with equities and motives in cyberspace.

In cyberspace, the vast majority of participants expressed that the rules of engagement are nascent and generally untested. Most participants described that decision-making uncertainty is complicated by the tradeoff decisions required between operational gain and intelligence loss. Many participants also stated that they perceived insufficient resources and national debate have been applied to cyber warfare concepts and capabilities. These participants added that these challenges are compounded by the lack of political resolve and insufficient transparency among interagency partners, especially within the intelligence community. Many participants considered response decisions following a cyber attack to be influenced heavily by the existing conflict posture. In addition, many were concerned that making the decision to respond could

appreciably increase the risk of escalating hostiles while unintentionally stimulating a cyber arms race.

Legal and Ethical Aspects

Nearly every participant described that the existing legal framework governing the use of force in cyberspace to be antiquated and inadequate to support military operations in an effective manner. Although essentially every participant expressed that cyber warfare is a completely ethical use of force, most conveyed that defining sovereignty and jurisdiction boundaries in cyberspace to be a challenging venture that complicates decision-making. Compounding these challenges, most participants noted that privacy, anonymity, and civil liberty concerns added complexity to the response decision process.

Most participants stated that the lack of practical definitions for hostile intent and hostile act in cyberspace made consistently responding to cyber attacks more difficult. While noting these definitional problems, many participants perceived that determining how to apply the laws of armed conflict in cyberspace to be problematic based on antiquated international treaties and the unpredictable nature of society's view of cyber warfare. Building on these considerations, many participants expressed compliance concerns with existing laws that already fail to provide effective governance and controls for malicious activities in cyberspace.

Organizational Concepts, Constructs, and Relationships

Essentially all participants described how the lack of collaboration and consensus, especially among the interagency, increased decision-making uncertainty following a cyber attack. Most participants clearly expressed how ineffective command and control

processes and ill-defined roles and responsibilities within existing cyber warfare organizational constructs considerably add to the complexity of response decisions. Many participants conveyed their perspectives on the situational need for both centralized and decentralized command and control structures when responding to the disparate cyber attack methods and source locations. In addition to this insight, several participants noted how the vast number of government stakeholders with conflicting equities in cyberspace complicates the synchronization and response decision process following a cyber attack. Some participants added that ambiguous leadership vision and weak accountability measures increase uncertainty when making response decisions.

Data, Information, and Technology Considerations

All but one participant described their inadequate understanding of current capabilities to be a substantial contributor to the uncertainty they experience when making cyber response decisions. Most participants expressed that the valuation and sharing of information is inconsistent, which complicates determining the impact of a cyber attack. Many participants further conveyed that inadequate information sharing results from a lack of access in addition to overly classified and compartmentalized tactics, techniques, and procedures. These challenges reduce situational awareness, which increase decision-making uncertainty.

Most participants explained that inadequate effort and priority have been placed on developing robust models and simulations designed to facilitate understanding the effects of cyber attacks. Several participants noted this problem is the result of insufficient research and development. Many participants found the widespread use of proxies and weak identification authentication measures make distinguishing between

criminal cyber activity and information warfare effects difficult. In addition, many remarked how immature forensic capabilities and data credibility challenges add complexity to making timely and effective response decisions. Several participants explained how the difficulties associated with determining data ownership and intellectual property rights considerably increase the uncertainty of legally responding to a cyber attack, especially when data servers reside in the United States.

Cyber Attack Characteristics

Almost all participants described that unintended higher order effects caused by responding to a cyber attack influences decision-making uncertainty. Most participants expressed that recognizing and categorizing the source and severity of a cyber attack to be very challenging. Adding to the complexity, most participants conveyed that understanding the motive and context of a cyber attack influences their response decisions and limits the development of an effective deterrence policy. Many participants thought improving the ability to express a cyber attack with equivalent kinetic attack characteristics would facilitate their response decision process. Additionally, many considered a better understanding of an adversary's cyber attack capacity (e.g., botnet size and scope) and precision (surgical strike characteristics) would improve their ability to respond. Because cyber attacks are often conducted in a covert manner, several participants stated that validating how the attack occurred to be extremely difficult, making response decisions untimely and uncertain.

Cyber Warfare Characteristics

Essentially every participant considered cyber warfare to be comprised of complex EBO well suited for self-defense and conducting counter responses even against

kinetic attacks. Further, most participants expressed they adamantly considered cyber warfare to be traditional military activity. However, many explained that determining how conventional rules of war apply in cyberspace to be challenging. Most added that deconflicting and synchronizing cyber operations to be complicated due to cumbersome planning and targeting processes further impeded by conflicting interagency equities. Several participants noted these problems hinder integrating and normalizing cyber warfare into mainstream military operations.

Because of undefined information valuation standards discussed earlier, many participants described that accurately conducting “battle damage” assessments following a cyber attack to be extremely difficult. In addition, many asserted their decision-making uncertainty was strongly influenced by the “fog of war” created in cyberspace resulting from advance deception capabilities and methods. Several added the complexity of cyber warfare is catalyzed by the low cost of entry into this domain (compared to traditional warfare), which provides an inexpensive medium for non-state adversaries to conduct attacks. Consequently, several participants concluded cyber warfare should be categorized as a type of irregular warfare from a doctrine perspective. Although several participants perceived an evolving level of readiness to respond to cyber attacks, they suggested a catastrophic cyber event (“Cyber 9/11”) may be required before interagency leaders or the general population seriously consider cyber warfare as a considerable threat to national security.

Cyberspace Characteristics

Nearly all participants described cyberspace as a ubiquitous domain of warfare embedded within a highly complex and chaotic environment. Further, most portrayed

cyberspace as an open and essentially boundaryless commons designed primarily as an interdependent communication medium. Most conveyed that these characteristics considerably contributed to their decision-making uncertainty following a cyber attack. Because most participants viewed the nation's critical infrastructure to be highly dependent on cyberspace, they readily expressed this ever-increasing dependency creates opportunities for insurgents as well as hostile and criminal activities. Many added the concept of cyberspace is complicated further by the duality of its virtual and physical nature. This inherent characteristic creates ambiguous cyberspace vulnerabilities and confounds understanding higher order effects when making response decisions. Several participants also considered the existing levels of network resiliency and security to be inadequate, making cyberspace vulnerable to increased attacks and malicious behavior.

Experience, Training, and Education Considerations

Most participants described their existing experience and expertise in cyber warfare for effectively making response decisions as insufficient compared to their skill levels in traditional warfare domains. Most attributed the lack of expertise to inadequate formal training opportunities during their career progression and the absence of cyber warfare curricula at higher-level DoD universities and educational institutions. Because of the nascent and burgeoning nature of cyber warfare, many participants expressed that current doctrine governing cyber warfare tactics, techniques, and procedures is undeveloped and not well understood. Exacerbating this problem is the lack of leadership support to develop and integrate realistic and challenging exercise scenarios into existing war games and simulations. Several participants conveyed that their lack of

experience results in poor anticipatory and proficiency skills with respect to making timely and effective response decisions following a cyber attack.

Structural Composite Description

The structural composite description was developed from the composite textual description using imaginative variation to discover underlying structural meanings and to capture the essence of the phenomenon. The structural composite description focuses on better understanding *how* the participants as a whole experienced *what* they perceived and described (Moustakas, 1994). The goal is to reveal structures “that are embedded in everyday experience, which can be grasped only through reflection” (Keen, 1975, p. 46). The structural composite description precipitates the feelings, thoughts, and beliefs of senior military officers, as a group, by exposing how they experience decision-making uncertainty following a cyber attack.

As a group, the participants represented senior military officers serving for the CJCS in cyber warfare divisions. Although all of the participants were well educated, holding multiple postgraduate degrees in most cases, only about half reported to their Joint Staff cyber division assignment with any formal information technology training, credentials, or special skills. The other half was traditionally trained as typical warfare officers within their respective Services and areas of expertise. Given their diverse backgrounds, age differences, and levels of leadership experience, the group’s feelings and insights converged on several key issues that were expressed adamantly and enthusiastically throughout the interviews. As senior military officers, they have been professionally developed within a culture of personal performance reflection, critical self-assessment, and causal analysis of underlying problems. Therefore, the composite

structures that emerged were presented from this perspective by keeping in mind the central research question they responded to during the interviews.

All of the participants felt their level of knowledge and understanding of cyber warfare required improvement. Although the group provided many reasons for their knowledge deficiencies, the vast majority believed they needed a much better understanding of the spectrum of response options available and the associated range of technical capabilities designed to accomplish a response order. Prevalent throughout the textual descriptions, the group recognized and described unresolved challenges with key definitions, declaratory positions on important policy issues, and frustration with an inadequate and antiquated legal framework. The group felt strongly that by defining response thresholds, hostile intent, and act of war in cyberspace using a common lexicon would reduce decision-making uncertainty. The participants shared that a national strategic policy was essential to provide vision and unity of effort across the interagency regarding cyber warfare initiatives. With the exception of the participants with legal credentials, the entire group firmly believed the limitations of the existing legal framework, laws, and treaties unnecessarily restricted legitimate, ethical warfare activities in cyberspace.

The group expressed strong feelings regarding the lack of collaboration and consensus by the stakeholder organizations with equities in cyberspace. Further, the majority of participants believed these organizations are too focused on intelligence gathering versus cyber operations and activities. Adding to these challenges, the group felt the interagency leadership has not firmly established suitable roles and responsibilities to conduct cyber warfare effectively. The participants largely thought

this problem has led to cumbersome command and control processes, ambiguous lines of authority, and overreliance on centralized organizational structures. The group clearly expressed that cyber warfare is effects-based and should be considered traditional military activity. The complexity of cyber warfare coupled with the ubiquitous, interdependent nature of cyberspace requires a better understanding of higher order effects in addition to more efficient deconfliction and synchronization processes. The group predominately felt that the necessary level of understanding would only result with continued experience gained by making cyber warfare decisions in conjunction with improved training and education opportunities.

Appendix O: Textual-Structural Synthesis

Textual-Structural Synthesis

The textual-structural synthesis is the final step in the phenomenological reduction and analysis process (Moustakas, 1994). During this step, the composite textual and structural descriptions were analyzed in order to develop a holistic depiction of the experience representing the group as a whole (Moustakas, 1994). By integrating the composite textual and structural descriptions using imaginative variation and reflective study as part of the synthesis process, the actualized meanings and essences of the phenomenon were more completely exposed and understood from a single vantage point.

The participants for this research study were senior military officers serving for the CJCS in cyber warfare divisions. Carefully selected and screened for their positions, the participants represented a group of extremely professional, highly motivated, and knowledgeable military officers with the responsibility of making complex response decisions. Specifically, the decisions made by the participants are at the national security level and are used to inform the CJCS, Combatant Commanders, the Secretary of Defense, and the President of the United States with COAs, military options, and recommendations following a cyber attack. Although the participants had diverse backgrounds, age differences, and levels of leadership experience, each participant was well trained and disciplined in the art and science of warfare. All of the participants viewed their roles as important and they expressed a strong desire to inform their profession. The senior officers openly and enthusiastically shared their perceptions and experiences as a means of improving existing decision-making processes.

An analysis of the composite textual and structural descriptions revealed consistent perceptual and experiential relationships between the key themes. The relationships were categorized into five distinct and interrelated components: response process, human factors, governance, technology, and environment. The *response process* component was supported by three key themes: response characteristics and efficacy considerations (Theme 1); cyber attack characteristics (Theme 7); and cyber warfare characteristics (Theme 8). The *human factors* component was supported by two key themes: social, behavioral, cultural, and cognitive aspects (Theme 2); and experience, training, and education considerations (Theme 10). The *governance* component was supported by two key themes: policy and strategic aspects (Theme 3); and legal and ethical aspects (Theme 4). The *technology* component was supported by one key theme: data, information, and technology considerations (Theme 6). The *environment* component was supported by two key themes: organizational concepts, constructs, and relational considerations (Theme 5); and cyberspace characteristics (Theme 9).

Response Process

The response process influences the decision-making uncertainty experienced by the participants following a cyber attack. The response process is comprised of a highly complex set of operations, activities, and events requiring an in-depth understanding and mastery of cyber warfare tactics, techniques, and procedures. Essentially all participants described their need to have a better understanding of the response options at their disposal including defined response thresholds (“red lines”) based on the laws of armed conflict. Because response thresholds (“lines in the sand of warfare”) are not properly defined, the participants described the decision-making process as unresponsive,

untimely, and ineffective. Most participants expressed the process to recognize and categorize the source and severity of a cyber attack to be lacking. Many participants thought improving the ability to express a cyber attack with equivalent kinetic attack characteristics would facilitate their response decision process. In addition, several participants stated that validating how the attack occurred to be extremely difficult, causing the response process to be untimely and uncertain.

Essentially every participant considered cyber warfare to be comprised of complex EBO conducted as traditional military activities and self-defense response processes. However, many explained that determining how conventional rules of war apply in cyberspace to be challenging. Most added that deconflicting and synchronizing cyber operations to be complicated due to cumbersome planning and targeting processes further impeded by conflicting interagency equities. Several participants noted these problems hinder integrating and normalizing cyber warfare into mainstream military processes. Many participants described the process of accurately conducting “battle damage” assessments following a cyber attack to be extremely difficult. In addition, many asserted their decision-making uncertainty was strongly influenced by the “fog of war” created in cyberspace resulting from advance deception capabilities and methods as compared to traditional warfare domains. Consequently, several participants concluded cyber warfare should be categorized as a type of irregular warfare from a doctrine perspective.

Human Factors

Human factors influence the decision-making uncertainty experienced by the participants following a cyber attack. Human factors include cognitive properties, social

behaviors, skills and abilities, organizational cultures, human-machine interaction, learnability, procedural usability, and decision-making among other related categories (Carroll, 1997). All participants described the need for an improved level of individual understanding regarding the complex dynamics, interrelated effects, and decision-making processes associated with cyber warfare. Most participants expressed that their inadequate level of understanding was limited by the lack of a common lexicon and an inconsistent vernacular, which are complicated by diverse values and belief systems from the numerous stakeholders with equities in cyberspace. Further, some participants added that their insufficient knowledge level negatively affected their self-confidence and ability to make sound decisions.

Most participants described their existing experience and expertise in cyber warfare for effectively making response decisions as insufficient compared to their skill levels in traditional warfare domains. Several participants conveyed that their lack of experience results in poor anticipatory and proficiency skills with respect to making timely and effective response decisions following a cyber attack. Most attributed their lack of expertise to inadequate formal training opportunities during their career progression and the absence of cyber warfare curricula at higher-level DoD universities and educational institutions.

Because of the emerging nature of cyberspace, many participants expressed that current doctrine governing cyber warfare tactics, techniques, and procedures is undeveloped and not well understood. Contributing to this problem is the lack of leadership support to develop and integrate realistic and challenging exercise scenarios into existing war games and simulations. Essentially every participant explained that

generational differences (i.e., cultural and ideological variances resulting from differences in age) added to the decision-making uncertainty. Regarding the social nature of cyberspace, several participants indicated that the existing international norms of behavior influence their decision-making process based on what is perceived as the acceptable bounds of response options. Many participants conveyed that *dehumanizing* cyber warfare (machine versus machine) would lessen the reluctance to respond to cyber attacks.

Governance

The governance structure influences the decision-making uncertainty experienced by the participants following a cyber attack. In this context, the governance structure is a system of rules, regulations, policies, laws, and traditions by which authority is exercised. Almost all participants had a perception that decision-making uncertainty is influenced strongly by an inadequate national strategic policy regarding cyber warfare. These participants asserted the lack of national policy limits the leadership's consideration of using cyberpower as a legitimate instrument of national power. Most participants explained that the inability to develop an effective cyber deterrence policy is compounded by countless actors with equities and motives in cyberspace. In cyberspace, the vast majority of participants expressed that the rules of engagement are nascent and generally untested. These participants added that these challenges are compounded by the lack of political resolve and insufficient transparency among interagency partners, especially within the intelligence community.

Essentially every participant described the existing legal framework governing the use of force in cyberspace as antiquated and inadequate to support military operations in

an effective manner. Although the participants strongly believed cyber warfare to be completely ethical, they noted that privacy, anonymity, and civil liberty laws considerably restrict the ability to respond to cyber attacks, especially in the absence of practical definitions for hostile intent and hostile act in cyberspace. While noting these definitional problems, many participants perceived that determining how to apply the laws of armed conflict in cyberspace to be problematic based on antiquated international treaties and the unpredictable nature of society's view of cyber warfare. Building on these considerations, many participants expressed compliance concerns with existing laws that already fail to provide effective governance and controls for malicious activities in cyberspace.

Technology

Technology influences the decision-making uncertainty experienced by the participants following a cyber attack. For this analysis, technology was considered information systems used to facilitate the practical application of knowledge. All but one participant described their inadequate understanding of current capabilities to be a substantial detriment to their decision-making process. Most participants expressed that information valuation models and standards to be immature, which complicate determining the impact of a cyber attack. Many participants conveyed that information sharing is severely limited due to unnecessary access restrictions and excessive classification requirements that reduce situational awareness and increase decision-making uncertainty. Most participants felt existing models and simulations designed to understand the effects of cyber attacks to be lacking due to insufficient research and development resources. Many participants found the widespread use of proxies and weak

identification authentication measures make attribution difficult. In addition, many remarked how immature forensic capabilities and uncertain data credibility/authenticity challenges complicated making timely and effective response decisions.

Environment

The environment influences the decision-making uncertainty experienced by the participants following a cyber attack. The environment is the system of interdependent settings, boundaries, conditions, objects, and circumstances that the participants interacted with when making response decisions. The environment is comprised of physical interfaces, organizational cultural factors, and virtually networked systems (i.e., cyberspace). Within their organizational environment, essentially all participants described how the lack of collaboration and consensus, especially among the interagency, complicated the decision-making process. Most participants clearly expressed how ineffective command and control processes and ill-defined roles and responsibilities within existing cyber warfare organizational constructs considerably add to the complexity of response decisions. Many participants discussed the situational need for both centralized and decentralized command and control structures when responding to cyber attacks originating within and outside areas of hostility. In addition, several participants noted how the various government stakeholders with conflicting equities in cyberspace complicated the synchronization and response decision process.

Nearly all participants described cyberspace as a ubiquitous domain of warfare embedded within a highly complex and chaotic environment. Further, most depicted cyberspace as an open and essentially boundaryless commons designed primarily as an interdependent communication medium. Many added cyberspace is characterized

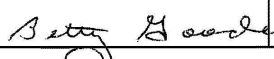

simultaneously by its virtual and physical nature. Most conveyed these inherent characteristics confounded understanding higher order effects when making response decisions and notably contributed to their decision-making uncertainty following a cyber attack. Because most participants viewed the nation's critical infrastructure as highly dependent on cyberspace, they readily acknowledged this ever-increasing dependency creates opportunities for criminal and hostile activities while enticing virtual insurgencies to be established. Several participants also considered the existing levels of network resiliency and security to be inadequate, making cyberspace vulnerable to increased attacks and malicious behavior.

Appendix P: Report Documentation Page

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.</p>					
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE		3. DATES COVERED (From - To)	
14-10-2010		Doctoral Dissertation		Feb 2008 - Oct 2010	
4. TITLE AND SUBTITLE Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Caudle, Daryl L.				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Phoenix, School of Advanced Studies 4615 E. Elwood Street Phoenix, AZ 85040				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of the Chairman of the Joint Chiefs of Staff 5000 Joint Staff Pentagon Strategic Plans and Policy (J5) Washington, D.C. 20318-5000				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) SR 10-00144	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for Unlimited Distribution					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT An essential element of the nation's comprehensive approach to cybersecurity is the ability for the Department of Defense to protect and defend its information enterprise. Unfortunately, decision-making uncertainty experienced by military leaders when determining the appropriate response to a cyber attack can impede cybersecurity efforts. This qualitative, phenomenological study was used to explore the perceptions and lived experiences of 21 senior military officers serving in cyber warfare divisions for the Chairman of the Joint Chiefs of Staff in Washington, DC. The synthesis of 10 key themes that were exposed during the phenomenological reduction analysis indicated that the decision-making uncertainty experienced by the participants following a cyber attack was described by five interdependent characteristics: (a) response process, (b) human factors, (c) governance, (d) technology, and (e) environment. These interrelated characteristics are similar to the factors found in the literature that describe organizational change uncertainty. The study further indicated the response decision-making process used by senior military officers following a cyber attack was best described by poliheuristic, noncompensatory decision theory.					
15. SUBJECT TERMS Cyberspace, cyber, use of force, cybersecurity, uncertainty, poliheuristic, decision-making, organizational change, phenomenological, response process, human factors, governance, technology, environment, cyberpower, deterrence, warfare, strategy, policy, legal framework, leadership					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			David A. Hoopes, LtCol, USAF
Unclassified	Unclassified	Unclassified	Unlimited	482	19b. TELEPHONE NUMBER (Include area code) (703) 697-2137

Reset

 Standard Form 298 (Rev. 8/98)
 Prescribed by ANSI Std. Z39.18
 Adobe Professional 7.0

REQUEST INFORMATION SHEET				SEE INSTRUCTIONS ON BACK	
TO: OFOISR ROOM 2C757, PENTAGON		1. TYPE OF REQUEST <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> APPEAL		This form is to be used for recording disclosure/ non-disclosure determination associated with processing a Freedom of Information or Privacy request.	
2. CASE NO. SR 10-00144		3. RECORD PROVIDED TO PROPONENT <input checked="" type="checkbox"/> FOR REVIEW?		4. COMPONENT SEARCH RESULTS <input type="checkbox"/> RECORD FOUND <input type="checkbox"/> NO RECORD	
5. - 8. RECORD DESCRIPTIONS					
5.a. DATE (YYYYMMDD)	b. SECURITY CLASSIFICATION U	d. ADDRESSEE		f. SUBJECT/TITLE Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers	
c. TYPE		e. ORIGINATOR			
6.a. DATE (YYYYMMDD)	b. SECURITY CLASSIFICATION	d. ADDRESSEE		f. SUBJECT/TITLE	
c. TYPE		e. ORIGINATOR			
7.a. DATE (YYYYMMDD)	b. SECURITY CLASSIFICATION	d. ADDRESSEE		f. SUBJECT/TITLE	
c. TYPE		e. ORIGINATOR			
8.a. DATE (YYYYMMDD)	b. SECURITY CLASSIFICATION	d. ADDRESSEE		f. SUBJECT/TITLE	
c. TYPE		e. ORIGINATOR			
9a. ACTION TAKEN BY COMPONENT <input type="checkbox"/> GRANT IN FULL <input type="checkbox"/> DENY <input type="checkbox"/> TRANSFER TO: <input type="checkbox"/> GRANT IN PART <input checked="" type="checkbox"/> NO OBJECTION TO DISCLOSURE				b. ADDRESSEE	
10. EXEMPTIONS INVOLVED FOR DENIALS (See 5 USC 552, 5 USC 552a, DoD Regulation 5400.7-R, and DoD Regulation 5400.11-R)					
11. RATIONALE FOR DENIAL					
12. REMARKS There is no objection to the release of the document.					
13. COORDINATION					
a. NAME (Last, First, Middle Initial)	b. OFFICE SYMBOL	c. TELEPHONE NO.	d. CONCUR	e. NON-CONCUR	
Hoopes, David A., Lt Col	AO (J-5)	697-2137	<input checked="" type="checkbox"/>		
14. ACTION OFFICER					
a. NAME (Last, First, Middle Initial)	b. RANK	c. TITLE	d. SIGNATURE	e. OFFICE TELEPHONE NUMBER	
Goode, Betty M.	Civ	Declassification Specialist		697-9962	
15. APPROVAL/DENIAL AUTHORITY					
a. NAME (Last, First, Middle Initial)	b. RANK	c. TITLE	d. SIGNATURE	e. DATE (YYYYMMDD)	
Richards, Douglas	Civ	Chief, Declassification Branch		2010 10 14	